Joint Committee on the Draft Investigatory Powers Bill

Written evidence

Access Now—written evidence (IPB0112)

Executive Summary

1. Thank you for this opportunity to provide comments. Communications surveillance interferes with individuals' human right to privacy, as well as other human rights recognised in international law and policies. Accordingly, laws that permit communications surveillance must respect certain standards, including necessity and proportionality. Additional principles are explained in the International Principles on the Application of Human Rights to Communications Surveillance.
2. Access Now applauds the UK Home Office for its attempt to provide public understanding of the scope of its investigatory powers and their application. However, we encourage the the Joint Committee on the Draft Investigatory Powers Bill to take notice of the substantial risk posed to human rights by its new and renewing authorities.
3. The Draft IP Bill threatens and fails to extend human rights protections, including those related to the right to privacy, protection of personal data, and freedom of expression. Portions of the Draft IP Bill risk undermining the integrity of communications systems through the weakening of encryption tools and technologies.
4. In addition to its impact on citizens and businesses of the United Kingdom, the Draft IP Bill will have a vast impact around the world, because some of the most invasive aspects of the draft will apply to individuals and providers outside of the UK. Accordingly, it will have deleterious effects on human rights of individuals around the world.[1]
5. In light of the risks posed by this draft, Access Now recommends key changes in conformity with human rights standards to protect security practices, increase oversight and transparency, and extend protections for non-nationals.

Access Now has also joined a coalition of civil society organizations in submitting Written Evidence broadly addressing the questions posed by the Joint Committee on the Draft Investigatory Powers Bill. These comments are intended to supplement the coalition comments.

I. About Access Now

1. Access Now is an international organisation that works to defend and extend digital rights of users globally.[2] Through representation in 10 countries around the world – including in the European Union - Access Now provides thought leadership and policy recommendations to the public and private sectors to ensure the internet's continued openness and the protection of fundamental rights. Our Technology Arm operates a 24/7 digital security helpline that provides real time direct technical assistance to users around the world.

[1] Secretary of State for the Home Department, Draft Investigatory Powers Bill (2015), Sections 69, 79, 189(8), and 31(3), available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf [Draft IP Bill].

[2] Access Now, https://www.accessnow.org.

2. Access Now previously participated in the consultative process led by Independent Reviewer of Terrorism Legislation David Anderson Q.C.,[3] as well as the consultative process instigated by the Home Office in 2015 in regard to the new Draft Equipment Interference Code of Practice and the updated Interception of Communications Code of Practice.[4] Access Now submitted Written Evidence on the Draft Investigatory Powers Bill to the technology issues inquiry[5] and the Joint Committee on Human Rights.[6] Access Now appreciates this further opportunity to input into the reform of UK surveillance law and practice.

II. International law and human rights

1. The United Kingdom is a party to the European Convention on Human Rights (hereinafter, the "ECHR"),[7] the EU Charter of Fundamental Rights (hereinafter, "the Charter"),[8] and the International Covenant on Civil and Political Rights (hereinafter, the "ICCPR").[9]
2. The ECHR and Charter establish the right to privacy (Articles 8 and 7, respectively) and freedom of expression (Articles 10 and 11, respectively). The European Court of Human Rights (hereinafter, the "ECtHR") has articulated the standards for each right. On the right to privacy, the ECtHR noted "[r]espect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings . . . "[10] On freedom of expression, the ECtHR noted that freedom of expression "protects not only the substance of the ideas and information expressed, but also the form in which they are conveyed."[11] The Charter also safeguards the right to protection of personal data, which the ECtHR articulated as an element of the right to privacy under the ECHR.
3. The ICCPR establishes the right to privacy (Article 17), the right to freedom of expression (Article 19), and the right to freedom of association (Article 22), among many others.
4. In a 2015 report, David Kaye, the United Nations Special Rapporteur for Freedom of Expression, explained that privacy and freedom of expression are tied to individuals' ability to use encryption and communicate anonymously.[12] Specifically, the Special

---

[3] Peter Micek and Ellie Lightfoot, *Access Contributes to Independent Review of UK Surveillance Abuses,* Access Now (Oct. 15, 2014), https://www.accessnow.org/blog/2014/10/15/access-contributes-to-independent-review-of-uk-surveillance-abuses.

[4] Jack Bussell, *Human Rights Left Out of Sight in UK's New Surveillance Guidelines,* Access Now (March 23, 2015), https://www.accessnow.org/blog/2015/03/23/human-rights-left-out-of-sight-in-uks-new-surveillance-guidelines.

[5] Access Now, *Written Evidence submitted by Access Now* http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25186.html

[6] Access Now and Fight for the Future, *Written Evidence from Access Now and Fight for the Future,* http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/human-rights-committee/legislative-scrutiny-draft-investigatory-powers-bill/written/25665.pdf

[7] European Convention on Human Rights, June 1, 2010, *available at* https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Convention_ENG.pdf.

[8] Charter of Fundamental Rights of the European Union, art. 8, 2000 O.J. (C 364); European Court of Human Rights *Personal data protection factsheet*, (Dec. 2015), http://www.echr.coe.int/Documents/FS_Data_ENG.pdf.

[9] International Covenant on Civil and Political Rights, Dec. 16, 1966, S. Treaty Doc. No. 95-20, 6 I.L.M. 368 (1967), 999 U.N.T.S. 171.

[10] *Rotaru v. Romania*, European Court of Human Rights (2002), *available at* http://hudoc.echr.coe.int/eng?i=001-58586.

[11] *Oberschlick v. Austria*, European Court of Human Rights (1991), *available at* http://hudoc.echr.coe.int/eng?i=001-57716.

[12] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Human Rights Council, U.N. Doc.A/HRC/29/32 (May 22, 2015) (by David Kaye).

Rapporteur found, "[e]ncryption and anonymity, today's leading vehicles for online security, provide individuals with a means to protect their privacy, empowering them to browse, read, develop and share opinions and information without interference and enabling journalists, civil society organizations, members of ethnic or religious groups, those persecuted because of their sexual orientation or gender identity, activists, scholars, artists and others to exercise the rights to freedom of opinion and expression."

5. The Universal Declaration of Human Rights (UDHR) and the International Covenant on Economic, Social, and Cultural Rights (ICESCR) both affirm the right to enjoy the benefits of science. The UDHR declares, "Everyone has the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits" (Article 27). The ICESCR recognises the right "to enjoy the benefits of scientific progress and its applications" (Article 15).
6. As part of the World Summit on the Information Society (WSIS), United Nations Member States, including the United Kingdom, agreed that "strengthening confidence and security in the use of ICTs for the development of information societies and the success of ICTs is a driver of economic and social innovation."[13] Further, "building confidence in the use of ICTs should be consistent with human rights."[14] Member States also noted concern over attacks against individuals and other entities undertaken through digital means.
7. The International Principles on the Application of Human Rights to Communications Surveillance provide a framework for protection of human rights against communications surveillance.[15] (hereinafter, "the Principles"). The Principles include Necessity, Proportionality, Legality, Transparency, Public Oversight, Integrity of Communications and Systems. The Principles' Preamble describes their utility:

   > *"Privacy is a fundamental human right, and is central to the maintenance of democratic societies. It is essential to human dignity and reinforces other rights, such as freedom of expression and information, and freedom of association, and is recognized under international human rights law. Communications surveillance interferes with the right to privacy among a number of other human rights."*

8. The Principles "apply to surveillance conducted within a State or extra-territorially."

1. Integrity of communications and systems

1. The Draft IP Bill may be interpreted to require operators to weaken or undermine encryption tools and technologies offered to internet users,[16] undermining human rights and the integrity of the internet. Another provision authorises the Secretary of

[13] Outcome Document of the High-Level Meeting of the General Assembly on the Overall Review of the Implementation of WSIS Outcomes, para. 53 (Dec. 14, 2015) http://workspace.unpan.org/sites/Internet/Documents/UNPAN95707.pdf.
[14] *Id.* at para. 55
[15] International Principles on the Application of Human Rights to Communications Surveillance, https://necessaryandproportionate.org.
[16] Draft IP Bill Section 51 (The Secretary of State can order providers to maintain a means to effectuate surveillance). More broadly, the Secretary of State may also order any telecommunications operator to take any steps that are considered necessary in the interests of national security. *Id.* at Section 188. Both of these authorities may be read broadly to give license to the Secretary of State to disrupt providers from offering the strongest encrypted services.

State to implement broad regulations that could place substantial burdens on providers and limit user security.[17]

2. The Guide to Powers and Safeguards, which prefaces the Draft IP Bill, states, "the draft Bill does not impose any additional requirements in relation to encryption over and above the existing obligations in the Regulation of Investigatory Powers Act (hereinafter, "RIPA")."[18] However, it is unclear that RIPA required providers to maintain "permanent intercept capabilities, including maintaining the ability to remove any encryption applied by the CSP."[19] Such authority was not anticipated in previous documents providing interpretation of existing surveillance authorities.[20]
3. The free development, distribution, access, and use of encryption protects confidentiality of communication, increases trust, helps prevent crime, and contributes to a healthy economy.[21] When used by organisers or legal defenders living under oppressive regimes, victims of domestic abuse, or journalists reporting on violent crime, encryption may even save lives.
4. Recently, many of the top cryptographic experts published a new report that explained that any exceptional access regime would "force a U-turn from the best practices now being deployed to make the Internet more secure," "substantially increase system complexity" and raise associated costs, and "would create concentrated targets that could attract bad actors."[22]
5. As stated above, encryption is at the heart of the free exercise of human rights like free expression and privacy, as guaranteed by the ICCPR, ECHR, and the Charter, as well as the right to benefit from scientific progress, affirmed in the ICESCR and UDHR.[23]
6. Encryption and anonymity enable freedom of expression. Any restrictions must *strictly* satisfy the conditions of ICCPR Article 19(3).[24] Per the Human Rights Committee, the only body charged with interpreting the ICCPR, governments must show "in specific and individualized fashion" that the restriction on expression is (1) provided by law, pursuant to one of the legitimate grounds, with sufficient precision and accessibility to provide notice and guidance; (2) necessary for a legitimate purpose; and (3) proportionate, meaning it is the "least intrusive instrument" available and not overbroad.[25] Applying that test, we find generally applicable restrictions such as mandatory backdoors or weakened security standards do not

[17] Draft IP Bill Section 189 (The Secretary of State may also issue regulations that obligate operators to ensure that they can assist with relevant authorisations.).
[18] The Guide to Powers and Safeguards, which prefaces the Draft IP Bill, states at para. 63, "the draft Bill does not impose any additional requirements in relation to encryption over and above the existing obligations in RIPA."
[19] *See, e.g.*, HOME OFFICE, *Interception of Communications Code of Practice Draft for Public Consultation* (Feb. 2015), *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/401866/Draft_Interception_of_Communications_Code_of_Practice.pdf [IC Draft Code of Practice].
[20] *Id*.
[21] Ryan Hagemann & Josh Hampson, *Encryption, Trust, and the Online Economy*, Nikanen Center (Nov. 9, 2015), https://niskanencenter.org/wp-content/uploads/2015/11/RESEARCH-PAPER_EncryptionEconomicBenefits.pdf.
[22] Harold Abelson et al., *Keys Under Doormats: mandating insecurity by requiring government access to all data and communications*, Massachusetts Institute of Technology Technical Report (July 6, 2015).
[23] *Encryption, Anonymity, and the "Right to Science"*, JUSTSECURITY (Apr. 28, 2015) https://www.justsecurity.org/22505/encryption-anonymity-debates-right-science.
[24] *Report of the Special Rapporteur on the protection and promotion of the right to freedom of opinion and expression* at para. 31.
[25] Human Rights Committee, *General Comment No. 34* (Sept. 12, 2011) http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

transparently provide notice to affected parties; are not imposed in a specific or individualised fashion; are not strictly necessary to achieve a legitimate aim; and do employ the least intrusive means, but rather result in a widespread, disproportionate, and indiscriminate impact.[26]

7. Limitations on the development or use of encryption subverts the right to benefit from scientific progress. The UN Committee on Economic, Social and Cultural Rights has also indicated that States party to the ICESCR "should prevent the use of scientific and technical progress for purposes contrary to human rights and dignity, including the rights to life, health and privacy . . ."[27] In the context of the Draft IP Bill, a number of technologies meant to conform to provisions on encryption, equipment interference, and filtering arrangements, among other, could be used to undermine human rights.
8. The Draft IP Bill could unilaterally place an affirmative, international obligation on providers, of which other governments, including repressive regimes, could take advantage and misuse to the detriment of human rights standards. This could also infringe on several ongoing domestic debates around the world. Several countries are currently in the middle of active debates on the topic of encryption, including India, where a draft policy proposal was recently withdrawn after technologists and experts objected that it would undermine privacy and secure communications,[28] and the United States.[29] Despite a public and open debate on encryption dating back to the 1970s,[30] the U.S. has repeatedly rejected any law or policy to undermine its development or use.[31]
9. While mandates to undermine encryption will harm human rights, the digital economy, and overall trust in the internet, they would do little to help investigate or protect against terrorism or other crimes. Criminals and terrorists would still have access to products that offer strong encryption, either by designing and building a new application or using one developed wholly outside of the UK. Instead, these mandates would likely have the biggest impact on innocent users seeking to communicate, transact business, and access information as part of everyday life, and who, in those interactions, would be denied access to the strongest security available and may be a bigger target for criminal actors.

<u>Recommendations</u>

---

[26] *Id.* at paras. 42-43.

[27] Economic and Social Council, *General Comment No. 17*, para. 35, U.N. Doc.E/C.12/GC17 (Jan. 12, 2006) http://www.un.org/Docs/journal/asp/ws.asp?m=E/C.12/GC/17.

[28] *India withdraws controversial encryption policy*, BBC News (Sept. 22, 2015), http://www.bbc.com/news/world-asia-india-34322118.

[29] Ellen Nakashima & Andrea Peterson, *Obama administration opts not to force firms to decrypt data - for now*, Washington Post (Oct. 8, 2015), https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data--for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699_story.html. *See also*, Mike Masnick, *Two of the most ridiculous statements from Senators at yesterday's encryption hearings*, TechDirt (July 9, 2015), https://www.techdirt.com/articles/20150709/00065731595/two-most-ridiculous-statements-senators-yesterdays-encryption-hearings.shtml.

[30] Henry Corrigan-Gibbs, *Keeping Secrets: Four decades ago, university researchers figured out the key to computer privacy, sparking a battle with the National Security Agency that continues today*, Stanford Magazine (Nov. 7, 2014), https://medium.com/stanford-select/keeping-secrets-84a7697bf89f#.lhngrmsud.

[31] *See, e.g.*, Nicole Perlroth & David E. Sanger, *Obama Won't Seek Access to Encrypted Data*, N.Y. Times (Oct. 10, 2015) ("F.B.I. director, James B. Comey, told the Senate Homeland Security and Governmental Affairs Committee that the administration would not seek legislation to compel the companies to create such a portal."), http://www.nytimes.com/2015/10/11/us/politics/obama-wont-seek-access-to-encrypted-user-data.html.

1. The Joint Committee on the Investigatory Powers Bill should clarify current obligations for providers related to the development and use of encryption.
2. The Home Office should not legislate in a manner that would require encryption back doors or key escrow or otherwise mandate exception access to user data. To do so would make millions, if not billions of users less safe and secure without impacting the ability of terrorists or criminals to use encryption tools, such as those they design themselves. This is supported by a recent petition to the U.S. President supported by dozens of civil society organisations, companies, and trade associations, and signed by over 100,000 individuals.[32]

2. Transparency and public oversight

1. The Draft IP Bill does not effectively ensure transparent surveillance procedures or meaningful public oversight, which are necessary to ensure government accountability and respect for human rights. Disclosures of statistics and relevant interpretations inform stakeholders, including policymakers, providers, and civil society, on the state of surveillance, and are essential to robust public discourse on the limits to liberty and privacy in the digital age.
2. The Draft IP Bill requires the publication of an annual report from the Investigatory Powers Commissioner, to include statistics on the use of surveillance authorities. The Prime Minister is free to redact any portion of the annual report for a broad spectrum of reasons, including national security.[33]
3. The Draft IP Bill fails to provide adequate public information on the interpretation of its key legal standards, namely necessity and proportionality. Public information about how authorities are applied is necessary in order that internet users have adequate notice of potential surveillance to which they may be subjected.[34]
4. While the Draft IP Bill provides for a Technical Advisory Board, it is limited to a consulting role in the review of the Secretary of State's notices and obligations.

<u>Recommendations</u>

1. The Draft IP Bill should be modified to specify that all novel or significant interpretations of the law by intelligence services, the Secretary of State, or other entities are made publicly available. The Draft IP Bill should be further modified to remove exceptions from the public reporting requirement on statistics related to surveillance, and should authorise granular reporting regarding what authorities are being used, how many users are targeted, and how many users are impacted by the exercise of those authorities.
2. The Draft IP Bill should grant operators the ability to disclose information, whether in specific, aggregate, or narrative form, about government requests related to communications surveillance. Operators should also be allowed to disclose any requests or pressure to hand over encryption keys, install or alter hardware or

[32] Dear President Obama, Stand up for Strong Security, https://savecrypto.org (last visited Nov. 26, 2015).
[33] Draft IP Bill Section 171.
[34] *See, e.g., Access Now et. al, Representations on Interception of communications and equipment interference: draft codes of practice* (Mar. 20, 2015), ("the risk of unnecessary or disproportionate surveillance pursuant to RIPA, ISA, and the Codes is so manifest, particularly in respect to bulk collection or large-scale, invasive equipment interference activities, that the authorisation, renewal, amendment, and oversight of the relevant warrants and authorizations should be entrusted to an entity independent of the bodies conducting the surveillance in order to ensure compliance with the ECHR."). *available at* https://s3.amazonaws.com/access.3cdn.net/6fa9a8bf795df015c5_7qm6bhsu4.pdf.

software, or to allow authorities access to facilities, networks, or data under their control.

3. The Draft IP Bill should be modified to specify that internet users are notified when their personal data is collected under the surveillance authorities, with enough time to enable a legal challenge and invoke other available remedies. Operators should also be permitted to provide this notice to their customers.
4. The Draft IP Bill should be modified to provide the Technical Advisory Board with independent standing and membership and imbued with all of the authorities and funding needed to operate independently.

3. Extraterritoriality

1. As discussed above, the Draft IP Bill grants the Secretary of State authority to issue regulations, including those relating to the removal of electronic protection, to persons outside the United Kingdom.[35]
2. In responding to the United Nations Human Rights Committee, the Government of the United Kingdom stated the position that the ICCPR has effect outside the territory of the State in "very exceptional cases."[36] However, the United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms considers States legally bound to provide equal protections for nationals and non-nationals, and noted "the use of mass surveillance programmes to intercept communications of those located in other jurisdictions raises serious questions about the accessibility and foreseeability of the law governing the interference with privacy rights, and the inability of individuals to know that they might be subject to foreign surveillance or to interception of communications in foreign jurisdictions."[37]
3. Mutual Legal Assistance Treaties (MLATs) facilitate the exchange of information relevant to an investigation between countries.[38] MLATs provide predictability and oversight, and frequently require respect for international human rights and domestic legal standards.[39] Ongoing government efforts aim to improve the MLAT system to ensure it meets the demand for the exchange of information across borders.[40] In the U.S., the President's' Review Group on Intelligence and Communications Technologies noted that support for the MLAT process demonstrates a commitment to "a well-functioning internet that meets the goals of the international community."[41]

<u>Recommendations</u>

[35] Draft IP Bill Section 189(8).
[36] U.N. Human Rights Committee (HRC), *UN Human Rights Committee: Sixth Periodic Report, United Kingdom of Great Britain and Northern Ireland*, 18 May 2007, CCPR/C/GBR/6, http://www.refworld.org/publisher,HRC,STATEPARTIESREP,GBR,46820b202,0.html para. 59.
[37] *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, General Assembly, U.N. Doc.A/69/397 (Sept. 23, 2014) (by Ben Emmerson).
[38] Mutual Legal Assistance Treaties, https://mlat.info/.
[39] *Id.*
[40] *See, e.g.,* U.S. Department of Justice, F.Y. 2015 Budget Request, http://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf.
[41] The President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World* 228 (Dec. 12, 2013), https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

- The extraterritoriality sections of the Draft IP Bill should be removed or clarified to limit their impact to the requirement for providers doing business within the UK to respond to valid court orders.
- The Draft IP Bill should apply the same standard to both citizens and non-citizens, and remove all areas where the law distinguishes either on virtue of citizenship or geographic location.
- The Draft IP Bill should re-assert a commitment to and support additional funding for the execution of MLATs, and foster reforms to update and strengthen the MLAT process.

4. Other issues impacting human rights

1. Access Now further identifies severe human rights problems with other provisions of the Draft IP Bill. For example, the Draft IP Bill fails to require advance approval of surveillance orders by an independent and competent judicial authority, fails to respect proportionality in its treatment of interference authorities, and fails to provide for adequate avenues of redress or to require that individuals are notified when they are subject to invasive surveillance that would interfere with their human rights in order that they would have an opportunity to challenge that surveillance in a court.
2. The Draft IP Bill authorises mandates for providers to retain personal data up to 12 months.[42] The Investigatory Powers Commission can also deem information or documents appropriate for retention.[43] Data retention mandates infringe upon individual privacy and chill the exercise of human rights including freedom of expression and freedom of association.[44] This infringement is particularly pronounced in situations without meaningful limits to the scope of the data that provider can be compelled to retain. The current Draft IP Bill does not contain any finding or evidence as to whether a legal review was conducted on whether – and how – these proposed measures were in conformity with rules articulated by the Court of Justice of the European Union (hereinafter, "CJEU").[45]
3. Filtering arrangements extend beyond existing powers and create new privacy and security risks.[46] The filtering arrangements considered in the Draft IP Bill are

[42] Draft IP Bill Section 71 (gives the Secretary of State authority to "require a telecommunications operator to retain relevant communications data if the Secretary of State considers that the requirement is necessary and proportionate [for an enumerated purpose]."). The retention order may provide for up to 12 months of data. *Id*. The Secretary of State may produce regulations that allow a provider to request a review of the retention order, at which point additional evidence may be taken. *Id*. However, pursuant to section 73, the Secretary of State is the ultimate arbiter of whether the retention order will stand following such a request. *Id.* at Section 73. Section 74 provides that data that is ordered retained must be secured and protected against accidental or unlawful destruction or unauthorised access, among other things. *Id.* at Section 74.

[43] Draft IP Bill Section 89(4).

[44] Letter from Access, et. Al. to Majority Leader Mitch McConnell, et. Al (May 11, 2015), *available at* https://s3.amazonaws.com/access.3cdn.net/ecffc6f83105be5bc5_8tm6bn51u.pdf. Other countries have recently considered and rejected data retention mandates. Ten EU countries invalidated data retention legislation in the aftermath of the CJEU data retention ruling, including Germany and the Netherlands In the United States, a proposal to include data retention mandates in the USA FREEDOM Act was rejected.

[45] *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others* (C-293/12) and *Kärntner Landesregierung and Others* (C-594/12), Court of Justice of the EU (8/4/2004), *available at* http://curia.europa.eu/juris/liste.jsf?num=C-293/12.

[46] Internet Service Provider's Association, *ISPA response to joint Committee on the draft Communications Data Bill* 2-6, http://www.ispa.org.uk/wp-content/uploads/ISPA-response-to-Joint-Committee-on-the-draft-Communications-Data-Bill.pdf.

overbroad in operation of compelled searches of private databases and may fail to meet requirements of legality, necessity, and proportionality.

4. Upon request, Access Now is available to provide further information on these invasions of human rights by the Draft IP Bill if it would so please the Committee.

Recommendations

1. Data retention mandates should not be promulgated in any form until the resolution of two relevant cases pending at the CJEU, Home Department v. David Davis and Tele2 Sverige AB v. Post-och Telestyrelsen (Case C-203/15).
2. The Draft IP Bill should be modified to provide explicit limits on the data that can be obtained under filtering arrangements, and to provide for explicit limits on storage and dissemination of that data.
3. Given the importance of this subject and the consequences on human rights and secure communications, the Draft IP Bill should be subject to careful scrutiny by Parliament and input to the UK government should be carefully considered. The Draft IP Bill should not be rushed through the pre-legislative process or other review.

5. Conclusion

1. Thank you for this opportunity to submit written evidence to this Committee.

21 December 2015

Access Now et al.—written evidence (IPB0109)

1. Thank you for this opportunity to provide comments. This written evidence is submitted on behalf of Access Now, Advocacy for Principled Action in Government, the Center for Financial Privacy and Human Rights, the Electronic Frontier Foundation, New America's Open Technology Institute, Restore the Fourth, and TechFreedom. We are human rights, technology policy, and civil society organisations based out of or doing work in the United States and internationally.

2. Communications surveillance interferes with individuals' human right to privacy, as well as other human rights recognised in international law and policies. Accordingly, laws that permit communications surveillance must be necessary and proportionate.

3. In particular, we note the close partnership between the surveillance agencies operating within the United Kingdom and the United States, as demonstrated by the string of investigative reports starting on June 6, 2013 and known colloquially as the "Snowden Revelations." While it is unclear the exact terms by which surveillance information is disseminated between the United Kingdom and the United States, it is clear that agencies in both nations work in close concert to conduct surveillance around the world. We know that information collected by UK intelligence agencies, including information about U.S. citizens and foreign nationals, is shared in secret with the U.S. National Security Agency to be held and analysed.47 Additionally, the extraterritorial effect of the Draft Investigatory Powers Bill means that its provisions are also likely to have direct impact on the signers of this Comment.

4. Accordingly, we recommend that the consideration of the Draft IP Bill be given adequate time, and not be rushed. Each provision should be provided with adequate attention and care. The surveillance authorities granted in the Draft IP Bill will subject millions, if not billions, of internet users around the world to surveillance by the UK intelligence and law enforcement agencies. In her introduction to the Draft Bill, the Home Secretary notes:

> *The draft Investigatory Powers Bill that has been published for pre-legislative scrutiny and public consultation builds on their recommendations to bring together all of the powers available to law enforcement and the security and intelligence agencies to acquire communications and communications data and make them subject to enhanced, consistent safeguards.*

47 Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies, & James Ball, *GCHQ taps fibre-optic cables for secret access to world's communications*, The Guardian (June 21, 2013), http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

5. However, the period for public consultation for the Draft, which numbers close to 300 pages including explanatory text and notes, has not given sufficient time to independently consider each provision as well as the interplay between separate authorities.

6. A new investigatory powers law must include suitably specific and clear authority as to give notice to the public of the circumstances when they may be subject to surveillance and provide for independent judicial review and robust human rights protections and safeguards, as well as transparency and accountability.

7. The Joint Committee on the Draft Investigatory Powers Bill (the "Draft IP Bill") has requested answers to several questions to inform its analysis of the draft bill. We provide answers in brief here. If you would like additional information, we encourage you to reach out to the signatories of this comment.

Overarching / Thematic Questions

Are the powers sought necessary? Has the case been made, both for the new powers and for the restated and clarified existing powers?

8. The International Principles on the Application of Human Rights to Communications Surveillance defines the standard of necessity:

> *Surveillance laws, regulations, activities, powers, or authorities must be limited to those which are strictly and demonstrably necessary to achieve a legitimate aim. Communications Surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights. The onus of establishing this justification is always on the State.*[48]

9. The European Court of Human Rights has explained that the secret surveillance authorities are amongst those that receive a greater level of scrutiny.49 The Home Office has not explained the necessity of the exceedingly broad surveillance authorities that it seeks to renew or instate in the Draft IP Bill. Rather, the Draft IP Bill appears to seek all foreseeable surveillance authorities, and grants their use with

48 International Principles on the Application of Human Rights to Communications Surveillance (May, 2014), https://en.necessaryandproportionate.org. [N&P]
49 *Klass v. Germany*, European Court of Human Rights, at para. 42 (1978), *available at* http://hudoc.echr.coe.int/eng?i=001-57510#{"itemid":["001-57510"]}.

little public oversight as to how the Secretary of State interprets their standards for use by the intelligence agencies, public agencies, or law enforcement agencies.

Are the powers sought legal?

10. *"The State must not adopt or implement a measure that interferes with these rights in the absence of an existing publicly available legislative act, which meets a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application."*50

11. The Draft IP Bill fails to provide this requisite level of clarity.51 Additionally, it fails to include a "sunset" provision that would require Parliament review the authorities granted periodically to ensure their continued need or the ability to incorporate additional safeguards.

Are the powers compatible with the Human Rights Act and the ECHR?

12. No -- nor are they consistent with the right to privacy even more deeply rooted in British traditions52 The Draft IP Bill violates several provisions of the European Convention on Human Rights ("ECHR"), including the Right to respect for private and family life (Article 8), Freedom of thought, conscience, and religion (Article 9), Freedom of expression (Article 10), and Freedom of assembly and association (Article 11), among others.

13. In a recent ruling of the European Court of Human Rights in the case *Roman Zakharov* v. *Russia*, the Court found Russia's system of secret interception of mobile telephone communications to interfere with Article 8 of the ECHR.53 The Court explained that, in order to be compatible with the ECHR, secret surveillance had to be clear on its face, supervised by a truly independent authority that is open to public scrutiny, and provide for notice and an opportunity to challenge the surveillance as soon as practicable.54 The Draft IP Bill is inconsistent with this standard.

50 N&P.
51 *Roman Zakharov v. Russia*, European Court of Human Rights (2015), *available at* http://hudoc.echr.coe.int/eng?i=001-159324.
52 Entick v. Carrington [1765] established a right to privacy in one's home from government intrusion. Malone v. Commissioner for the Metropolitan Police [1976] admitted the legality of government wiretapping of telephones, but set out requirements for the legality of wiretapping that are not met by a system of before-the-fact and universal surveillance for police purposes.
53 *Id*. at para. 235.
54 European Court of Human Rights, *Q & A Roman Zakharov v. Russia, Grand Chamber judgment*, (Apr. 12, 2015), http://www.echr.coe.int/Documents/Press_Q_A_Roman_Zakharov_ENG.PDF.

Is the requirement that they be exercised only when necessary and proportionate fully addressed? Are they sufficiently clear and accessible on the face of the draft Bill?

14. We appreciate the Draft IP Bill's application of the "necessary and proportionate" standard, but the bill should specifically define these terms in accordance with international human rights law and policy.55 Bulk collection is fundamentally inconsistent with the "necessary and proportionate" standard. Further, the Draft IP Bill fails to provide for transparency into, or independent judicial approval of, the Secretary's interpretation and application of those standards. Finally, the purposes for which surveillance can be "necessary and proportionate" are also overbroad, for example, "to assist investigations into alleged miscarriages of justice," which is also facially unclear as to what activities would be covered.

Is the legal framework such that CSPs (especially those based abroad) will be persuaded to comply?

15. No. Communications Service Providers (CSPs) must be given the ability to respect the rights of their users and to object to government orders that interfere with those rights. The Draft IP Bill fails to provide for sufficient mechanisms for CSPs to appeal overbroad or objectionable orders and fails to give CSPs sufficient rights to inform users of orders that implicate their personal information. CSPs risk being sued in their own states for complying with these orders if they are not consistent with local law. Additionally, provisions requiring extra-territorial application of broad authorities -- including those that may require the removal of electronic protections of user data, such as encryption -- are particularly troubling and may make it harder for both large and small companies to protect their users.

Are the powers sought workable and carefully defined? Are the technological definitions accurate and meaningful (e.g. content vs communications data, internet connection records etc.)?

16. As explained above, the Draft IP Bill fails to provide adequate clarity as to the authorities that it authorises, and for many provisions the authorities described are over-broad and lack adequate transparency or oversight. In addition, the definitions are inadequately precise.

17. For example, the broad definition of what constitutes "communications data," and, in particular, an "internet connection record," fails to consider either the level to

55 N&P.

which collection of internet records is invasive or the substantially different process that must be taken for collecting that information versus obtaining telephone communications data. The line between communications content and communications data on the internet is not clear, and authorities to collect internet connection records must take this into account.

18. The powers of bulk and targeted equipment interference, specifically described in statute for the first time in this Bill, is granted with a broad set of permitted targets, and with no limits on technical scope or consideration for the effect on the services of CSPs required to comply with the warrants, nor the effect on their customers' security and privacy.56

Does the draft Bill adequately explain the types of activity that could be undertaken under these powers?

19. No. Several provisions of the Draft IP Bill fail to adequately define the different activities that the Secretary could authorise public agencies, law enforcement agencies, or intelligence agencies to pursue under their authority. Additionally, several provisions of the bill contain a broad and undefined "catch-all" which authorises or requires from third-parties, "any conduct which it is necessary to undertake in order to do what is expressly authorised or required" by the warrant—including, for example, "the interception of communications not described in the warrant."57

Is the wording of the powers sustainable in the light of rapidly evolving technologies and user behaviours? Overall is the Bill future-proofed as it stands?

20. While the language of a law should indeed be "technology neutral" in order to protect against developments that render its provisions inadequate or irrelevant, the Draft IP Bill goes too far by providing inadequate definitions of key terms, including internet connection records, and overbroad and unspecific authorisations, including the provisions on filtering. In addition, provisions that compel CSPs to tamper with their own infrastructure in order to provide "technical capabilities" place no external limits on what new capabilities might be might be imposed on service providers58. The bill's targeted equipment interference provisions places an ad hoc obligation on providers to comply with individual demands from the intelligence services, military

56 See submissions to this Committee by the Electronic Frontier Foundation, Open Technology Institute , Center for Democracy and Technology, and others.
57 Secretary of State for the Home Department, Draft Investigatory Powers Bill (2015), §§ 12(5), 81(5), 106(5), 122(7),135(4) and 188(3), *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf [Draft IP Bill].
58 Draft IP Bill § 189.

intelligence or law enforcement to transform or even undermine the functionality of their service,59 with no oversight by the IP Bill's own Technical Advisory Board, or possibility for CSPs or their customers to challenge these secret changes.

Are the powers sufficiently supervised? Is the authorisation process appropriate? Will the oversight bodies be able adequately to scrutinise their operation? What ability will Parliament and the public have to check and raise concerns about the use of these powers?

21. The Draft IP Bill fails to provide for adequate supervision or oversight of the provided-for authorities. In fact, the provided-for level of review is far below even the perfunctory review provided by the Foreign Intelligence Surveillance Court ("FISC") in the United States, a body that has received international criticism for its secret deliberations and decisions despite its independence. Responding in part to this criticism, the U.S. Congress recently increased the transparency and accountability of the FISC, providing for unclassified publication of substantial Court decisions and the appointment of *amicus curiae* to provide additional independent legal or technical expertise. No equivalent resources or requirements are provided for the judicial commissioners or the Investigatory Powers Commissioner.

Selected Specific Questions

Interception

Are there sufficient operational justifications for undertaking (a) targeted and (b) bulk interception?

22. The targeted interception envisioned by the Draft IP Bill is already far from the layman's definition of "targeted," and may include not only a person, organisation, or single set of premises,60 but may also include "a group of persons who share a common purpose or who carry on, or may carry on, particular activity," as well as "more than one person or organisation, or more than one set of premises, where the conduct authorised or required by the warrant is for the purposes of the same investigation or operation."61 With this, already very broad, authority to conduct interception, it is not clear why additional "bulk" authority is necessary, or why the additional safeguards for bulk cannot or should not be applied to the "targeted" interception. Bulk interception violates core privacy rights guaranteed in

59 Draft IP Bill § 101.
60 Draft IP Bill § 13(1).
61 Draft IP Bill § 13(2).

international law.62 Bulk interception is inherently disproportionate and its authorisation and, as implemented in the Draft IP Bill, would have excessive impact on people outside of the UK.63

Is the proposed process for authorising urgent warrants workable?

23. The Draft IP Bill allows the unilateral approval of a warrant, without the approval of a judicial commissioner so long as the person who issues the warrant considers that an urgent need exists in order to do so. This is an inadequate and inadequately specific standard, and the decision as to whether or not a situation is "urgent" is not subject to any judicial review.64 This process fails to provide sufficient human rights protections or adequate oversight.

Data Retention

Do the proposed authorisation regime and safeguards for bulk data retention meet the requirements set out in the CJEU Digital Rights Ireland and the Court of Appeal Davis judgments?

24. The Draft IP Bill authorises mandates for providers to retain personal data up to twelve months.65 The Investigatory Powers Commission can also deem information or documents appropriate for retention.66 Data retention mandates infringe upon individual privacy and chill the exercise of human rights including freedom of expression and freedom of association.67 This infringement is particularly pronounced in situations without meaningful limits to the scope of the data that provider can be compelled to retain. The current Draft IP Bill does not contain any finding or evidence as to whether a legal review was conducted on whether – and how – these proposed measures were in conformity with rules articulated by the Court of Justice of the European Union (hereinafter, "CJEU").68

62 *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, General Assembly, U.N. Doc.A/69/397 (Sept. 23, 2014) (by Ben Emmerson).
63 Draft IP Bill § 106.
64 Draft IP Bill § 20.
65 Draft IP Bill § 71 (gives the Secretary of State authority to "require a telecommunications operator to retain relevant communications data if the Secretary of State considers that the requirement is necessary and proportionate [for an enumerated purpose]."). The retention order may provide for up to 12 months of data. *Id*. The Secretary of State may produce regulations that allow a provider to request a review of the retention order, at which point additional evidence may be taken. *Id*. However, pursuant to section 73, the Secretary of State is the ultimate arbiter of whether the retention order will stand following such a request. *Id.* at Section 73. Section 74 provides that data that is ordered retained must be secured and protected against accidental or unlawful destruction or unauthorised access, among other things. *Id.* at § 74.
66 Draft IP Bill § 89(4).
67 Letter from Access Now, et. al. to Majority Leader Mitch McConnell, et. al (May 11, 2015), *available at* https://s3.amazonaws.com/access.3cdn.net/ecffc6f83105be5bc5_8tm6bn51u.pdf.
68 *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others* (C-293/12) and *Kärntner Landesregierung and Others* (C-594/12), Court of Justice of the EU (8/4/2004), *available at* http://curia.europa.eu/juris/liste.jsf?num=C-293/12.

Equipment Interference

Should the security and intelligence services have access to powers to undertake (a) targeted and (b) bulk equipment interference?

25. "Equipment interference" carries with it the implication that the power is restricted to impeding normal equipment operations, but may also include adding unexpected new functionality to a device. Under targeted and bulk equipment warrants, telecommunication providers must obey any instructions given by or on behalf of the person to whom the warrant is addressed, and are bound by a gag order, which prevents them from conferring with others before executing the orders given by the warrant holder.69 The broad scope of machine interference warrants, the range of affected providers who may be compelled to assist, and the large set of potential targets, make this power one of most potentially intrusive in the new bill. Yet it lacks many of the review and oversight mechanisms attached to other, narrower powers.

Are the safeguards for such activities sufficient?

26. Not even remotely. Given the Draft IP Bill's weak oversight provisions, these powers would undermine trust in a broad range of online services, technology companies, academic research, and government services.

Oversight

Would the proposed Judicial Commission have sufficient powers, resources and independence to perform its role satisfactorily?

27. Under the Draft IP Bill, the judicial commissioners would not be fully independent of the Executive—the same entity whose authorities will be responsible for conducting much of the surveillance authorised by the Draft IP Bill. The commissioners would be appointed by and serve at the pleasure of the Prime Minister. Additionally, the head judicial commissioner, known as the Investigatory Powers Commissioner ("IPC"), would be given the power to remove other judicial commissioners unilaterally (in consultation only with the Prime Minister) on grounds that are not set out in the legislation.70

69 Draft IP Bill § 102.
70 Draft IP Bill § 168(6)-(7).

Are the new arrangements for the Investigatory Powers Tribunal including the possibility of appeal adequate or are further changes necessary?

Even the limited oversight provided for by the judicial commissioners is undermined by the grant of authority for the IPC to review final decisions of a judicial commissioner that fail to approve a sought-after warrant.

Conclusion

28. This comment is signed by Access Now, Advocacy for Principled Action in Government, the Center for Financial Privacy and Human Rights, the Electronic Frontier Foundation, New America's Open Technology Institute, Restore the Fourth, and TechFreedom.[71]

21 December 2015

71 If you have any additional questions or inquiries, you can send them to Amie Stepanovich at AccessNow.

ADS—written evidence (IPB0083)

ABOUT ADS

ADS is the premier trade association advancing the UK's Aerospace, Defence, Security and Space industries. ADS comprises over 900 member companies across all four sectors, with over 850 of these companies identified as Small and Medium Size Enterprises. Together with its regional partners, ADS represents over 2,600 companies across the UK supply chain.

The UK is a world leader in the supply of aerospace, defence, security and space products and services. From technology and exports, to apprenticeships and investment, our sectors are vital to the UK's growth – generating £56bn a year for the UK economy, including £31bn in exports, and supporting 800,000 jobs.

INTRODUCTION

1. ADS is the national industry body for the UK's security industry, covering the full range of capability areas relevant to national security and resilience. It also provides the Secretariat for the UK's Security and Resilience Industry Suppliers Community (RISC). RISC was formed in 2007 at the instigation of the Home Office to act as the principal channel of communication between the Office for Security and Counter Terrorism (OSCT) and security sector. It is an alliance of the national, regional and capability-specific industry groupings representing the sector as well as academia.

2. Academic RiSC is an umbrella alliance of 26 universities specialising in security-related research. It was founded in 2014 at the instigation of the Home Office with the aim of promoting the engagement of academia with industry and government on issues of national security.

3. ADS and Academic RiSC have established a group of technical experts from Primes, SMEs and academia to provide input to the Government on the development of the Investigatory Powers Bill. The group has expertise from a range of disciplines.

4. The aims of the group are to:

    - Provide technical advice on certain capabilities in scope of the Bill.
    - Ensure the Bill remains, as far as possible, technologically neutral and that it is able to cater for rapid developments in technology (in line with considerations related to necessity and proportionality).
    - Ensure legal clarity and public confidence in the development and use of capabilities provided by the security sector.

KEY RECOMMENDATIONS

5. **Recommendation 1:** That Government works with technical experts from the security sector in order to further understand the financial impact of decisions made, the risks

associated with them and the limitations and capabilities of different current and future technologies.

6. **Recommendation 2:** That HMG considers the below key questions in the development of the codes of practice. Work should also be undertaken alongside the security sector to test and adjust the codes of practice and remove ambiguities prior to implementation.

7. **Recommendation 3:** That HMG specifies that the Investigatory Powers Commission has embedded, qualified security sector technical specialists to inform strategy, planning and decision making as well as raising the technical awareness of others within the IPC

8. **Recommendation 4:** That HMG considers a timescale of between 5 and 7 years to re-visit the legislation

RESPONSE TO RELEVANT QUESTIONS

Are the powers sought workable and carefully defined?

9. The powers as they currently stand are workable as long as they are properly resourced. The key decisions which have to be made are:

- Level of security required by CSPs when storing data
    - Physical security of site
    - Vetting of staff
    - Training of staff
    - Technical decisions on level of protection of data (isolation from other networks, encryption etc.)

- Will the Bill enable better cooperation with CSPs and, even if CSPs do provide the data required of them, will this meet all of the requirements of law enforcement and intelligence agencies given the proliferation of OTT services, end-to-end encryption etc? If not, there may be an increased demand for intrusive techniques such as Equipment Interference (EI) technologies and interception. This will place greater demand on the security sector to develop and produce equipment to a scale that they have not in the past.

- What will the performance requirements be for technologies developed for particular purposes
    - Will there be “acceptable failure rates” for products (1 error in 10,000 data records? 1 error in 1,000?)

10. HMG will also have to consider whether they want to develop ‘sovereign capabilities’ in certain areas. This will require consideration of the practicalities and commercial implications of maintaining technologies developed in the UK for HMG use only.

11. These decisions should be made in consultation with the security sector (including both academia and industry) in order that decisions are informed by and grounded in an accurate understanding of existing and future capabilities within the fast-evolving technological environment and a thorough understanding of the commercial implications.

12. **Recommendation 1: That Government works with technical experts from the security sector in order to further understand the financial impact of decisions made, the risks associated with them and the limitations and capabilities of different current and future technologies.**

Are the technological definitions accurate and meaningful (e.g. content vs communications data, internet connection records etc.)?

13. The definitions of content and communications data in the Bill are the most developed. The definition of Internet Communication Records still needs further work. For example:

- Would ICRs actually help identify the originator and the true end destination?
- Do records need to contain data volumes?
- Over what period – second by second or minute by minute - do ICRs need to be collected?

14. Questions have been raised by CSPs in evidence sessions for the Joint Committee on the draft Investigatory Powers Bill and the Science and Technology Committee as to the practicality of the ICR concept. For example:

- Whether the Bill will require CSPs to maintain a record of user activity on over the top (OTT) services, requiring CSPs to be provided by the intelligence agencies with probing and EI capability in order to collect this data
- Whether the ICR concept is so unrecognisable to CSPs and such a significant departure from the way that data is currently collected, that totally new data collection practices will have to be introduced, adding huge costs

15. This group would disagree with both of these contentions.

16. Firstly, it is not our understanding of the Bill that CSPs will have to probe or intrude on users OTT activities if they were hidden from the CSP. This would be the preserve of the law enforcement and intelligence agencies. As mentioned above, this necessitates greater clarity around where the bulk of activity in the implementation of the Bill is likely to lie.

17. Secondly, the ICR concept may be different in minor ways from the current system of data collection and storage, but the technical experts on this group have stated that collecting data in this way is certainly doable. Depending on the specific detail and requirements for the collection process (see above) costs could vary but the technologies necessary to collect data in this way could be developed with relative ease.

18. However, it is worth noting that the security sector has some doubts that the concept of the ICR will continue to be relevant over the coming years as universal encryption becomes commonplace and the data that flows over CSPs becomes more inaccessible.

19. Perhaps more importantly, the definitions need to be supported by a useful set of examples within the Codes of Practice in order to provide the security sector with clarity as to how investigative techniques and technologies might be applied by law enforcement and intelligence agencies.

20. **Recommendation 2: That HMG considers the above questions in the development of the codes of practice. Work should also be undertaken alongside the security sector to test and adjust the codes of practice and remove ambiguities prior to implementation.**

Is the wording of the powers sustainable in the light of rapidly evolving technologies and user behaviours?

21. It is not possible to achieve sustainability solely through the wording of the powers. In order to ensure the powers are sustainable, the Bill should build a framework, outlining the considerations that can be applied to a range of investigative techniques and technologies. The legislation itself should act as a set of parameters, describing the information that different agencies are legally allowed to seek, under what circumstances and the limits on the level of intrusion permitted in order to achieve this. The codes of practice sitting beneath the legislation should be updated in light of the developing technological backdrop and should act as the drivers of implementation.

22. This is broadly how the legislation is currently structured and this group supports this. Successful implementation will require:

- The appropriate expertise to be in place and the appropriate individuals to be empowered in the right way, including security sector technology specialists
- The appropriate level of oversight to ensure that the codes of practice and their use remain within the limits and spirit of the law
- Keeping the Codes of Practice under constant review and updated as and when necessary

23. This group would advocate for a number of the individuals within the Investigatory Powers Commission to have expertise in the development of security technologies. This is in order to ensure that strategy, planning and decisions are informed by a thorough understanding of the limitations and capabilities of technology. Technical experts in industry are recognised through technical qualifications and the IPC should consider whether to use a similar system to ensure that they have sufficient technical experts on which they can draw.

24. **Recommendation 3: HMG to specify that the IPC has embedded, qualified security sector technical specialists to inform strategy, planning and decision making as well as raising the technical awareness of others within the IPC**

Overall is the Bill future-proofed as it stands?

25. Despite the fact that, as described above, the structure of the Bill is right, with the pace of technological evolutions that we have seen over the last decade and this development becoming ever faster, it is hard to see legislation of this nature lasting more than 7 to 10 years. The first smart phone was only introduced 8 years ago but they are now ubiquitous. The emergence of quantum computing and the ever-growing internet of things are likely to lead to further significant paradigm shifts which may, in turn, lead to new considerations for the intelligence and law enforcement agencies.

26. The fundamental concepts that the legislation is built on - ICRs, communications data, equipment interference and Communications Service Providers – are likely to move, develop and change significantly over time. For example:

- Many question whether CSPs will still play the same role and be structured in the same way in the future. Increasingly CSPs simply act as 'dumb pipes', transferring data that they cannot process or understand
- There are also questions as to whether IP addresses or metadata will persist in a form that we would recognise today

27. This does not necessarily mean that the legislation is not viable or needs revolutionary change. It simply means that it is likely to have a shelf life. It can be sustained through technical support to the IPC and regular updating of the codes of practice as discussed above. However, there are likely to be such significant shifts in the technological landscape over the next few years leading to fundamental changes to the threat as well as the capabilities of law enforcement and intelligence agencies, that it will be necessary to revise the law again in the not too distant future.

28. **Recommendation 4: HMG to consider a timescale of between 5 and 7 years to re-visit the legislation**

Will the oversight bodies be able adequately to scrutinise their operation?

29. Please see recommendation 3.

CONTRIBUTING COMPANIES AND INSTITUTIONS

Imperial College, London
Royal Holloway, University of London
Southampton University
Cambridge University
BAE systems
Raytheon
QinetiQ
Praetor Consultants Limited
Repknight

ADS Group
Blue Lights Digital
Forensic Analytics
Surevine

21 December 2015

Amberhawk Training Limited—written evidence (IPB0015)

12 December 2015

Introduction

1. This submission is primarily limited to the bulk personal dataset powers in Part 7 of Draft Investigatory Powers Bill ("***the Bill***") and other Parts of the Bill to the extent that they concern the processing of personal data (e.g. Part 3 deals with communications data that are also personal data – or "communications personal data").

2. My evidence assumes that bulk personal data collection powers will remain after the Committee has delivered its verdict; it thus suggests that a new structure that can introduce badly needed safeguards that are additional to the "double lock" (about which I make no comment and which I also assume will be maintained in any future Bill). The structure revolves around a new approach to the Data Protection exemption that applies for safeguarding national security and which has not changed since 1984.

3. In summary, I hope to show that **the Committee can assert that the Data Protection Act should become the prevailing mechanism that applies to the processing of personal data by the national security agencies**. In essence, this Bill updates the powers available to these agencies, but fails to update the protections afforded by the Data Protection Act. This is the major oversight addressed in my evidence.

4. The key changes that are needed to update the protection for individuals ("data subjects") and organisations are outlined below. They are:

    i. A separation between the Investigatory Powers Commissioner and the Judicial Commissioners to avoid a conflict where the Investigatory Powers Commissioner investigates himself or a judicial colleague.

    ii. The ability for organisations and data subjects to use an appeal system with respect to any warrant that requires the processing of bulk personal dataset for a national security purpose; for this to work, the separation in (i) above has to occur as it allows for an independent review of the warrant authorisation procedure.

    iii. A statutory Code of Practice that applies the Data Protection Principles to the processing of personal data for the purpose of safeguarding national security (rather than some proposed "Ersatz Principles" which in my view create a significant risk of "mission creep").

    iv. Detail on how the national security exemption (in section 28 exemption of the Data Protection Act) can be updated from the 1984 Act position; in summary, the exemption is applied when each warrant is sought or renewed and is specific to the warrant.

    v. The role of the Investigatory Powers Commissioner in regulating the Data Protection Act and the powers needed by the Commissioner to deliver

effective protection for data subjects and protection for organisations subject to the powers in the Bill.

vi. For Government to clearly identify how Article 8 of the Human Rights Act is complied with; this is important given the Government's commitment to replace the Human Rights Act.

vii. A "sunset clause" on different Parts of the Bill, so the powers can be refreshed by Parliament in the context of future technological advances (e.g. the Internet of things); to do otherwise would leave a risk that broad based powers can be inappropriately used to legitimise activities that really should need Parliamentary approval.

viii. The removal of all powers that provide an alternative avenue to collect bulk personal data.

5. The protection afforded to data subjects by the Data Protection Act should be available even though the processing of personal data is for a very sensitive purpose. This is because "*the nature of the set is such that **it is likely that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service** in the exercise of its functions" (definition of a bulk personal dataset: Clause 150(1)(b)of the Bill; my emphasis).* Additionally, I suspect much communications personal data will also relate to many individuals who also prove to be of little interest to the national security agencies.

6. In short, if data subjects are "*unlikely to become of interest to the intelligence service"* then their personal data should be afforded, wherever possible, the full protection of the Data Protection Act by the Bill. My evidence shows how this protection can be delivered.

7. The Principles in the Data Protection Act have passed the test of time in establishing a balance between the need to process personal data for a controversial purpose and the protection of the interests of the individual concerned. For example, if the police and all their sensitive criminal intelligence collections of personal data about the Mafia can learn to co-exist with these Principles, without "mishap", for nearly three decades (since the 1984 Act), one cannot see why communications personal data or a bulk personal dataset held by the national security agencies should be any different, especially if the data subjects are "*unlikely to become of interest to the intelligence service".*

8. Since 1984, the national security function has been largely exempt from data protection considerations, as a wide exemption from the Data Protection Act applies whenever personal data are processed for safeguarding national security (Section 28 of the DPA). Evidence that this exemption applies can require a certificate to be signed by the Secretary of State; however this certificate, unlike a warrant, is only signed if or when it is needed.

9. Section 28 certificates appear to be timeless. This is illustrated by the Investigatory Powers Tribunal case involving Privacy International in October last year *([2014] UKIPTrib 13_77-H; delivered on 05/12/2014, paragraph 19*). In statements made to

the Tribunal, the barrister for GCHQ produced a certificate signed by David Blunkett thirteen years previously (in 2001) to show that key obligations in the Data Protecting Act were exempt.

10. It is my evidence that application of the Data Protection Act in the way I suggest below could help mitigate concerns about the proportionality of collecting bulk personal datasets or mass communications personal data. This implementation applies the requirements of the Act to the national security purpose, it updates how the exemption for safeguarding national security is applied, and makes the Investigatory Powers Commissioner the regulator who exercises the powers in the Act. It does not jeopardise the national security function.

11. The changes I suggest allows the Investigatory Powers Commissioner to:

    a. look into the detail of the processing of personal data for safeguarding national security purposes;

    b. deal with complaints from data subjects or data controllers;

    c. sort out proportionality problems associated with the processing of personal data. and

    d. where necessary enforce the appropriate data protection standards.

12. It is my contention that the changes I suggest establish a robust set of counterbalancing protections for data subjects and for those organisations that provide bulk personal datasets. **In a data protection sense, the Bill affords the opportunity to bring the national security agencies in from the cold**; **this opportunity should be taken**.

The Investigatory Powers Commissioner must be separate from the Judicial Commissioners.

13. My first comment relates to the Investigatory Powers Commissioner; this post has to be completely separate from the Judicial Commissioners who approve the warrants. **The Committee should consider recommending a separation between the Investigatory Powers Commissioner and the Judicial Commissioners.**

14. The Bill does not achieve any separation. Indeed, Clause 167(6) states that "*The Investigatory Powers Commissioner is a Judicial Commissioner and the Investigatory Powers Commissioner and the other Judicial Commissioners are to be known, collectively, as the Judicial Commissioners*".

15. If there is not a complete separation between the Investigatory Powers Commissioner and the Judicial Commissioners, then the Government's chosen regulatory body is likely to be investigating the consequences of its own decisions. For instance, how is the Investigatory Powers Commissioner to meet the obligation in clause 169(3)(a) to *"keep under review the acquisition, retention, use or disclosure of bulk personal datasets by an intelligence service*" without investigating

the consequences of his own warrant authorisation decision as a Judicial Commissioner (or any other Judicial Commissioner)?

16. In the context of national security and because personal data relates to a "*majority of the individuals are not, and are unlikely to become, of interest to the intelligence service*" the lack of separation inherent in the Government's proposals could easily undermine public confidence in the double lock protection, irrespective of the changes I suggest. This is likely to be the case, when in future, you have something akin to the Snowden revelations and an Investigatory Powers Commissioner investigating his own decision as a Judicial Commissioner.

17. As will be seen (at paragraph 41 below), separation is important to the success of the improvements I suggest. I also suggest that this separation will introduce an element of independence that will reassure the public about the collection of bulk personal datasets.

The Bill as drafted does not explicitly protect personal data

18. With respect to Part 7 of the Bill (the bulk personal dataset (BPD) provisions), paragraph 74 of the Bill's preamble (which appears under a heading "*What safeguards will there be*?") states that "*A statutory Code of Practice will set out additional safeguards which apply to how the agencies access, store, destroy and disclose information contained in the BPDs*". The BPD Code is proffered as a safeguard in addition to the "double lock".

19. However, in Schedule 6 which concerns all Codes or Practice, there is no detail as to what should appear in the BPD Code of Practice. **The Committee may wish to press for detail as to the content of the BPD Code as the safeguards appear to be no more than a blank canvass to be completed by the Secretary of State once a future Bill becomes law.** One cannot criticise the safeguards in the BPD Code if there is no Code or relevant provisions to make comments about!

20. However, the mere existence of this BPD Code of Practice means that the Government is anticipating the continuation of an unchanged wide Section 28 exemption in the Data Protection Act with respect of bulk personal datasets in favour of the Code (when its content is eventually published) – even though the personal data collected relate to data subjects of no interest to the national security agencies.

21. With respect to the processing of communications personal data in Part 3, there is another Code of Practice applying; the content of this Code is specified in Schedule 6, paragraph 3. Paragraph 3(2)(a)-(2)(f) contains what I would describe as "Ersatz Principles" (which do not apply to bulk personal datasets).

22. The Ersatz Principles in Schedule 6, paragraph 3(2)(a)-(2)(f) are as follows:

> "(*a) why, how and where the data is held,*
> *(b) who may access the data on behalf of the authority,*
> *(c) with whom, and under what conditions, the data may be disclosed,*

(d) the processing of the data for purposes otherwise than in connection with the purposes for which it was obtained or retained,

(e) the processing of the data together with other data,

(f) the processes for determining how long the data should be held and for the destruction of the data".

23. These Ersatz Principles are phrased in a permissive way, unlike the Data Protection Principles. Clearly the intended function of these Ersatz Principles is to reassure the public; however, to the contrary, they fall well short of offering any significant protection.

24. For example, the Second Principle in the Data Protection Act requires that any personal data obtained for specific purpose(s) should not be further used or disclosed for an "*incompatible purpose*". By contrast, the Ersatz Principles (c) and (d) could allow for far wider uses/disclosure purposes by the national security agencies as the word "*incompatible*" is missing. Indeed any consideration of the "*purpose*" of any disclosure, which is crucial to several Data Protection Principles including the Second Principle, is absent from Ersatz Principle (c).

25. The Fifth Principle requires that personal data "*shall not be kept for longer than is necessary for that purpose or those purposes*"; the Ersatz Principle (f) clearly omits consideration of the "*purpose*" of retention and is inferior for that reason.

26. In general, these Ersatz Principles should be replaced by the Data Protection Principles that have protected data subjects for decades. In my view (and this comment might be uncharitable), the Ersatz Principles are not designed to protect the data subject; they are there to facilitate further processing (perhaps function creep) on the part of the national security agencies.

27. The Committee should assert that the Ersatz Principles in Code should be exchanged for the Data Protection Principles and that the Data Protection Principles should be central to all Codes relating to the processing of personal data.

How the Section 28 exemption in the DPA should apply

28. Clearly, there will be a need for exemptions from some provisions in the Data Protection Act that apply to safeguarding national security. I now show that the exemption can be wholly incorporated as part of the warrant arrangements and this step offers real safeguards for data subjects through a separate Investigatory Powers Commissioner.

29. In summary, the national security exemption is applied to the acquisition of bulk personal datasets or communications personal data ***when the agencies apply for each warrant (or on warrant renewal***) from the Secretary of State and a Judicial Commissioner.

30. Thus, instead of timeless certificates that are signed once, the exemption is applied for **each operation** at the warrant level (or on renewal or warrant) and at the time of the operation. In this way, consideration of the exemption from the provisions of the Data Protection Act becomes an additional protection to that of the judicial double lock. For example, the Judicial Commissioner and Secretary of State are able to consider issues such as further use, retention, lawfulness, accuracy, fairness and exemption from rights as part of the warrant approval process. In other words, the application of the Principles becomes central to the warrant authorisation process.

31. Residual Section 28 certification under the Data Protection Act may still be necessary for circumstances not covered in the Bill (e.g. there are limited to case-by-case exemptions that are necessary for the safeguarding of national security in any particular investigation). However, these certificates too should become time limited (e.g. 1 year before any renewal) and each application of this exemption should be covered by a certificate. The Investigatory Powers Commissioner should be able to review **all** aspects of the processing of personal data relating to such certificates even if they do not relate to personal data obtained from the use of powers in the Bill.

32. The enforcement regime (including Monetary Penalty Notices) in the Data Protection Act should apply to bulk personal dataset and communications personal data; such powers can be exercised by the Investigatory Powers Commissioner established by the Bill. The national security agencies right of Appeal against the exercise of powers by the Commissioner can be to the Investigatory Powers Tribunal.

33. This means that the Investigatory Powers Commissioner can obtain information about the processing of personal data, enforce the Data Protection Principles, consider the application of the national security exemption in detail, consider the rights of data subjects, and in the worst case scenarios, fine the national security agency if there is a serious transgression.

34. There is no risk to national security arising from such a safeguard but the fact that the data subject can seek redress via the Investigatory Powers Commissioner makes such redress accessible (unlike the current legalistic and costly appeal to the Investigatory Powers Tribunal).

35. The Assessment Notice power in Section 41A of the Data Protection Act to permit a data protection audit should be extended to apply to national security agencies in the context of bulk personal dataset and communications personal data processed by these agencies. If any Audit is undertaken by the Investigatory Powers Commissioner established by the Bill; there is no risk to national security arising from such a safeguard.

36. The Data Protection Act provisions with respect to data sharing should be applied. This usually means that any new data sharing has to be accompanied with a full Privacy Impact Assessment and can be subject to investigation by the Investigatory

Powers Commissioner if need be. In general, there is no Privacy Impact Assessment accompanying this Bill even though most data subjects are not of interest to the national security agencies.

37. The data protection standards with respect to national security should be applied whenever personal data are acquired by the authorities. For example, clause 46(7)(a) of the Bill refers to obtaining personal data that are "*in the interests of national security*" which is lower than the data protection standard of obtaining personal data that is for "*safeguarding national security*".

38. Similarly clause 46(7)(b) refers to obtaining being "(*b) for the purpose of preventing or detecting crime*" when the data protection standard is that the person making the disclosure to the authorities has to be satisfied that "*failure to disclose would prejudice prevention and detection of crime*". (As a point of clarification; the more protective Data Protection Act provisions deal the exchange of personal data from the standpoint of the organisation making the disclosure; the draft Bill views the exchange from the standpoint of the authorities obtaining the personal data – however it is the same personal data that are being exchanged).

39. All the changes above would reassure the public that not only are the checks and balances at the warrant signing stage (the double lock), there could be independent checks on the subsequent processing of a bulk personal dataset and communications personal data at any time. The mechanism to trigger the checks and balances are available to data subjects and data controllers who have to provide the bulk personal data.

40. By contrast, there are no penalties for failing to apply the Code(s) of Practice that describe the processing of a bulk personal dataset and communications personal data and the only real checks occur when the warrant is signed or renewed. Indeed, there is no role for the Investigatory Powers Commissioner with respect to the Data Protection Act.

The role of the Investigatory Powers Commissioner

41. For the above to be successfully implemented, clause 169 should provide the Investigatory Powers Commissioner with the following powers and obligations to enforce the application of the Principles and where appropriate, rights of data subjects.

    I. The Investigatory Powers Commissioner should exercise powers in the Data Protection Act with respect to bulk personal datasets and communications personal data in the same way as the Information Commissioner does in relation more normal personal data. Where the Investigatory Powers Commissioner exercises powers, these can be appealed to the Investigatory Powers Tribunal.

    II. The Investigatory Powers Commissioner has no role in handling or investigating complaints from data subjects. As the majority of data subjects

are "*not of interest*" to the intelligence services, the Commissioner should be able to consider complaints directly from them.

III. Organisations that are required to provide bulk personal dataset and communications personal data should be able to raise a formal complaint to the Investigatory Powers Commissioner that the warrant or authorisation approved by a Judicial Commissioner provides for disproportionate data sharing (i.e. organisations should have the right to ask for a review of a warrant/authorisation procedure if they have concerns over proportionality). To avoid prejudicing an operation, disclosure should first occur; however, any disclosed personal data should be destroyed if the Investigatory Powers Commissioner arrives at the same conclusion as the complainant (subject to appeal to the Investigatory Powers Tribunal).

IV. Consideration should be given for organisations and data subjects to appeal to the Investigatory Powers Tribunal against a failure of the Investigatory Powers Commissioner to find in favour of the applicant (using a process that was established for the Freedom of Information Act).

V. The Investigatory Powers Commissioner has no role in assessing whether bulk personal dataset and communications personal data, once approved under the warranting arrangements, have proved to be useful. The Commissioner ought to be able to establish Key Performance Indicators that demonstrate that bulk access is worthwhile (with the implication that if access is not worthwhile, the warrant becomes void and the datasets destroyed) and impose reporting requirements with respect to those Indicators on the national security agencies.

VI. All bulk personal dataset holdings should be reported to the Investigatory Powers Commissioner as well as the Secretary of State; this should be on the face of the Bill. This step will ensure the Commissioner knows the extent of bulk dataset collections and will be able to comment on these in his annual report, and where necessary exercise powers with respect to such personal data

VII. The Investigatory Powers Commissioner should have a role in supervising all Section 28 certificates under the Data Protection Act and ensuring there is no cross over with respect to powers in this Bill. (I have already stated that each application of the Section 28 exemption should be covered by a certificate which lasts a year to enable the certificate to be reviewed).

VIII. With respect to communications personal data obtained by authorisation (under clause 46 of the Bill), any authorisation has to describe why access is both necessary, proportionate and requires the application of any exemption in the Data Protection Act. The Investigatory Powers Commissioner should be able to define what detail he needs to be described and retained when authorisation occurs and what detail is needed to substantiate the use of each exemption in the Data Protection Act. The Investigatory Powers Commissioner should have the power to negate the application of any

exemption in any particular case. Note: because of the range of organisations involved with clause 46, there might be a number of exemptions in the Act that might apply that have nothing to do with safeguarding national security.

IX. Data matching across any combination of bulk personal datasets should be considered in the context of any data sharing to other bodies of the product of data matching. However, intended or actual data sharing and data matching should be identified in an authorisation, or on a warrant, or on warrant renewal, or reported to the Investigatory Powers Commissioner when a warrant lapses. The intent here is to allow the Investigatory Powers Commissioner to compile a complete picture of these activities and be able to investigate any data sharing or data matching arrangements.

X. The Investigatory Powers Commissioner can ensure that there is a commitment, as far as possible, to transparency with respect to bulk dataset acquisition/communications personal data. Such transparency already occurs without harm to national security. For instance with respect to Police & national security access Congestion Charge ANPR data, the TfL website states[72]:

> *"In 2012 the Mayor of London's Crime Manifesto included a commitment to instruct TfL to give the Metropolitan Police Service (MPS) direct real time access to the Automatic Number Plate Recognition (ANPR) cameras we use to enforce our Road User Charging schemes, for the purposes of preventing and detecting crime…..*
>
> *….**This was an expansion of a pre-existing arrangement with the MPS established in 2007, under which they were given access to TfL's ANPR data specifically for the purpose of using it to safeguard national security**. This arrangement was approved by the Home Secretary, who signed a certificate confirming that TfL, and the MPS, are exempt from certain provisions of the Data Protection Act 1998 for that purpose." (my emphasis).*

XI. The above shows that it is possible to be more transparent about the application of the Data Protection Act and the obtaining of personal data for their functions as clearly, if TfL's statement had jeopardised an operation, then the national security agencies would have asked for it to be removed.

Comments on Article 8 of the Human Rights Act

42. The Committee should recognise the Government is asking Parliament to accept that Article 8 of ECHR allows the national security agencies to collect bulk personal dataset and communications personal data when there is no prior suspicion with respect to the vast majority of data subjects. The legal advice that the Government has relied on to substantiate Article 8 compliance should be published so that this

[72] https://tfl.gov.uk/corporate/privacy-and-cookies/road-user-charging

issue can be debated properly; at the moment, compliance with Human Rights obligations is asserted without evidence.

43. This is especially important as there might be changes to Article 8 that arise from the Government's review of the Human Rights Act, and of course, the purpose of the draft Bill procedure is to allow for such an informed debate.

44. **There should be a "sunset clause" on Part 7 of the Bill as Parliament needs to review the legislation in the context of future technological developments that will result in further bulk personal datasets being created (e.g. Internet of things, smart metering, ANPR datasets**).

45. Parliament should learn from the abuse of process that arose by reliance on Section 94 of the Telecommunications Act 1984[73]. There are significant risks to allow wide ranging bulk data collection powers being left active for decades to come, to be used in any context, on any personal dataset, related to any future technology that might emerge.

46. I recommend **to the Committee a similar sunset clause in relation to communications personal data (Part 3) and to other Parts of the Bill.**

47. The Government wants the public to accept that the bulk collection of personal data does not breach their Article 8 rights without seeing the detail that justifies this course of action; such a leap of faith could be more palatable if the safeguards I suggest here were to be adopted.

48. **It should be a matter of policy that the more invasive the powers to interfere with private and family life, the stronger the powers of the Commissioner are to ensure that such powers are not misused**. Currently, with respect to the national security function, there is an inverse policy applying: the stronger the invasive powers, the weaker the protection for individuals. Sadly the proposals in the Bill continue the latter philosophy.

Removal of other powers to obtain personal data

49. All existing powers (i.e. other in the Bill) that could be used by the national security agencies to obtain a bulk personal dataset or communications personal data should be negated. For example, Schedule 1 of Counter-Terrorism Act 2008 which modifies the "Representation *of the People (England and Wales) Regulations 2001 (S.I. 2001/341*)" is not repealed. This modification includes Regulation 108A which is entitles the "*Supply of full register etc to the security services*". Not to close down existing powers would mean that there may be a secondary access route that could allow access to personal data outwith the protections in this Bill.

[73] The national security agencies have relied on pre-internet legislation (the Telecoms Act 1984) to legitimise activities that were never debated in Parliament. As the technology changed Government should have authorised in these activities in any anti-terrorism law from 2001 or indeed RIPA. This is evidence of a clear reluctance to engage with Parliament on these difficult issues.

50. The powers to obtain bulk personal dataset are not limited in any way whatsoever; this means that bulk databases of medical records can become targets for acquisition. The Bill, however, protects privileged communications data, **the Committee should consider whether, for example, medical records need to be protected from the operation of the bulk dataset provisions**. If so, I recommend the inclusion of a defined set of databases that cannot be obtained in bulk and a general provision in the Bill that allows the Secretary of State to identify the bulk personal datasets that are protected.

51. Finally, there is a risk that the national security agencies could become a repository of bulk personal datasets that other public bodies can use. This risk is enhanced especially if the Data Protection Principles are exempted by wide ranging certificate under and unchanged Section 28 exemption (and if something like the Ersatz Principles appear as part of the BPD Code of Practice).

About myself

52. I have been a data protection practitioner for 30 years and am a founder member of Amberhawk Associates and a Director in Amberhawk Training Limited since the company was founded in 2008. The company specialises in training staff who are responsible for data protection, Freedom of Information, and information security and other aspects of Information Law.

53. In 2012, I was appointed to two Government Advisory Committees. I am a member of the Identity Assurance, Privacy and Consumer Advisory Group (advising the Cabinet Office on "privacy friendly" use of identity assurance techniques and on data sharing) and the Data Protection Advisory Panel (advising the Ministry of Justice on its approach to the EU's Data Protection Regulation and Directive in the field of law enforcement).

54. I have given oral and written evidence before various Parliamentary Select Committees where issues of privacy, data protection and security have arisen (e.g. ID Cards, Surveillance, Computer Misuse Act, data retention policies, supervision of the national security agencies). I have also been asked to give a presentation to European MEPs when the European Parliament was discussing the proposed Data Protection Regulation.

Dr C. N. M. Pounder;
Amberhawk Training Limited;

14 December 2015

Amnesty International UK—supplementary written evidence (IPB0074)

Summary of Recommendations in this Submission:

Amnesty International UK recommends:

1. that bulk surveillance powers contained in the draft Bill, including bulk interception warrants, be excised from the UK statutory regime. Further, that the broadly defined thematic warrants under the targeted warrants regime be amended to conform with the UK's human rights obligations, e.g. cover more specific categories of persons and include the need for reasonable suspicions of wrongdoing.

2. that the Draft Bill be amended to provide a clear, accessible framework governing intelligence sharing that ensures, inter alia, it is as limited as possible for permissible purposes, and does not include receiving or sending the product of bulk surveillance or material obtained through human rights abusive methods.

3. that the authorisation process be amended so that (i) decisions to authorise warrants are taken by an independent judicial body following the application of (or with the interim non-statutory approval of the application by) the Secretary of State, or through a similarly full judicial authorisation process. (ii) Such a decision would require full disclosure of all relevant materials underlying the application. (iii) To the extent the decision to authorise the warrant has to be made without the knowledge and presence of the person concerned, it should also involve the participation of a designated person challenging the request and advocating for the protection of human rights and fundamental freedoms.

4. that the oversight mechanisms be revisited in their entirety to ensure proper safeguards against abuse.

5. that provisions for special protection for sensitive professions be included in the body of the legislation, and include human rights NGOs.

Introduction

1. Amnesty International UK welcomes the opportunity to input into the work of the Committee. However we wish to express our serious concern at the speed of this consultation process. After several promises from the government that the draft Bill would proceed at a sensible pace with sufficient time for proper consultation and scrutiny, Amnesty International UK is disappointed to be given less than 7 weeks for that process and to see that the Committee is expected to complete its work and report in very little more. Our view is that this is woefully inadequate time for a Bill of this level of complexity and length. It raises serious questions about the much vaunted government commitment to openness in this difficult sphere.

2. As such, we focus this submission on a small number of issues (addressed below under the Committee's specific questions, **grouped and highlighted in bold**) and have not

sought to address all the questions in the Call for Evidence that we might have wished had there been more time allowed. The failure to mention something in this submission should not be read as an indication that it is not of concern. We hope this submission will nevertheless be useful to the Committee.

Amnesty International UK

3. Amnesty International UK is a national section of a global movement of over seven million supporters, members and activists. We have over 600,000 supporters in the United Kingdom. Collectively, our vision is of a world in which every person enjoys all of the human rights enshrined in the Universal Declaration of Human Rights and other international human rights instruments. Our mission is to undertake research and action focused on preventing and ending grave abuses of these rights. We are independent of any government, political ideology, economic interest or religion.

4. Amnesty International Ltd. has been engaged in litigation challenging the UK government over the mass (or 'bulk') interception of communications under the existing statutory regime, as well as over the regime governing the sharing of intelligence between the USA and the UK in relation to communications intercepted under USA surveillance programmes. That litigation has resulted *inter alia* in (a) a judgment that in the view of the Investigatory Powers Tribunal the existing regime is 'in accordance with the law' for the purposes of articles 8 and 10 ECHR; (b) a further judgment that government intelligence sharing with the USA was unlawful prior to disclosures made during the litigation; and (c) that Amnesty International itself has been the victim of unlawful surveillance activity (following what the Tribunal considered to be lawful and 'proportionate' interception and accessing of the communications under a general – bulk – warrant). The case, which groups ten human rights organisations from four continents, is currently before the Strasbourg Court and may therefore have a significant bearing on the subject matter of this Bill.

5. The IPT's findings regarding the UK government's surveillance of human rights organisations provides one example of what overbroad surveillance powers lead to. We hope that the Committee will have high in its mind the global reverberations not only of that kind of activity, but of legislation of this kind. As part of an international movement, Amnesty International UK is acutely aware of how important the UK's actions are in making a statement to the international community about what is and is not acceptable in the realm of surveillance and other interferences with human rights.

Bulk interception and human rights: Has the case been made, both for the new powers and for the restated and clarified existing powers? Has the case been made, both for the new powers and for the restated and clarified existing powers? Are there sufficient operational justifications for undertaking (a) targeted and (b) bulk interception?

6. There is no question that interception and examination of individuals' personal communications (whether of content or communications data) is an interference

with a range of human rights[74]. As such, the interception itself must be 'in accordance with the law', necessary and proportionate if it is to be lawful. Amnesty International UK considers that indiscriminate mass surveillance is never a proportionate interference with the rights to privacy and freedom of expression (articles 8 and 10 ECHR) and can thus never be lawful under the Human Rights Act 1998 and/or ECHR. The interception, analysis or other use of communications in a manner that is neither targeted nor based on a reasonable suspicion that an individual or specific location is sufficiently closely linked to conduct that must legitimately be prevented, is disproportionate.

Bulk interception warrants

7. The Draft Bill would place on a statutory footing a bulk surveillance regime permitting unbounded state interception of all communications in selected network bearers, the application of selectors to those communications, and the unlimited selection from those communications of particular data for further access and examination. Bulk interception warrants, provided for in chapter 1 Part 6, purport to allow this activity primarily ('*main purpose*' in the draft Bill, see clauses 106 and 107) with regard to '*overseas related communications*' as well as for '*operational purposes'* which may be of a *'general'* nature (see clauses 106, 107 and 111). Such broadly drawn provisions and absence of any requirement for reasonable suspicion and other sufficient safeguards against abuse will enable the inherently disproportionate interference with billions of private communications in a routine manner.

8. It is clear from recent Strasbourg cases, in particular the Grand Chamber judgment in *Roman Zakharov v Russia*[75] -- which concerned a similar state capability to access communications in bulk – that enabling legislation for interception must, *inter alia*, (i) clearly indicate what kind of events and activity amounting to threats to national security or serious crime might lead to interception based on reasonable suspicion [see paras 185, 245-248, 260]; and (ii) ensure that interception warrants *'clearly identify a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorisation is ordered. Such identification may be made by names, addresses, telephone numbers or other relevant information'* [see para 264].

9. As such, a Draft Bill which provides for warranted blanket, untargeted interception for any of a range of broadly defined purposes (there is no definition of 'national security' or a threat to it in the Bill), and whose required operational purpose may even be cast in terms of "*general purposes*" (clause 111(4)), cannot satisfy the UK's human rights obligations. Such authorisations grant the kind of "*very wide discretion*" to the state that the Strasbourg Court has confirmed is open to abuse[76].

[74] *Klass v Germany* 6 September 1978, Series A No 28 at §41; *Weber and Saravia v Germany* ECHR 2006 XI at §77; *Kennedy v United Kingdom* 26839/05 18 May 2010 at §118, *Malone v United Kingdom* 2 Aug 1984, Series A No 82 at §84

[75] European Court of Human Rights, *Roman Zakharov v Russia,* app no. 47143/06, Grand Chamber, Judgment of 4 December 2015, available at http://hudoc.echr.coe.int/eng?i=001-159324

[76] *Zakharov*, para 267

'Targeted' interception warrants

10. The system which the draft Bill characterises as 'targeted' warrants also gives cause for concern. It is similarly based on broad terms such as 'national security', and lacks any requirement for reasonable suspicion that the target is connected with specific national security threats or serious crimes. The provision for broader thematic warrants under the guise of a so-called targeted warrants regime indeed shades into bulk collection. Clause 13 suggests, *inter alia*, that communications of a potentially wide and unspecific segment of the population could be subjected to the so-called 'targeted warrants' regime. For instance, phrases such as "*a group of persons who share a common purpose or who carry on, or may carry on, a particular activity*" are not specific enough to satisfy the requirements of human rights law.

11. Further, even if contrary to the above such broad categories were lawful, they would then appear significantly to undermine or obviate entirely any suggested justification for the bulk interception warrants under Chapter 1 Part 6: if such broad groups of people can lawfully be the subject of a targeted interception warrant, what is the legitimate reason for indiscriminately intercepting the communications of entire segments of the domestic and overseas population?

12. ***Amnesty International UK recommends that bulk surveillance powers contained in the draft Bill, including bulk interception warrants, be excised from the UK statutory regime. Further, the broadly defined thematic warrants under the targeted warrants regime should be amended to conform with the UK's human rights obligations, e.g. cover more specific categories of persons and include the need for reasonable suspicions of wrongdoing.***

<u>Intelligence sharing:</u> Are the powers compatible with the Human Rights Act and the ECHR? Is the requirement that they be exercised only when necessary and proportionate fully addressed? Does the draft Bill adequately explain the types of activity that could be undertaken under these powers? What ability will Parliament and the public have to check and raise concerns about the use of these powers? Does the draft Bill allow the appropriate organisations, and people within those organisations, access to communications data?

13. Despite its very significant human rights implications, there is little to no proper reference to intelligence sharing with overseas authorities in the Draft Bill (outside of MLATs). That is particularly surprising in light of the attention given to this subject – particularly to the sharing of the product of bulk interception - in the recent IPT litigation, brought by Amnesty International and other NGOs, referred to above. Amnesty International believes that any international sharing of material obtained through communications surveillance, solicited or otherwise, must occur in accordance with a human rights compliant framework – the first step being to have a clear statutory framework. That framework must further ensure that human rights abuses do not result from any such sharing.

14. Without this, such activity cannot be human rights compatible. In particular, it cannot be said to have a proper legal basis and be necessary and proportionate. If

there is no clear statutory framework then the Committee's questions as to whether parliament and the public will have the ability to check and to raise concerns about these activities and powers can only be answered in the negative. Nor can it be said that the draft Bill allows the appropriate organisations to have access to communications material, since we will not know how this works at all outside the UK.

15. In respect of sharing material that is obtained by the UK with overseas authorities, clause 39 (entitled "*Interception in accordance with overseas requests*" but otherwise making little reference to its subject matter) makes very general provision for interception carried out in response to a request "*in accordance with a relevant international agreement*" but with no explanation as to what those agreements may be – presumably secret arrangements which the public (and/or parliament) therefore are not aware of. It is an extremely broad enabling provision that cannot begin to be sufficiently clear to satisfy the UK's human rights obligations in this field. It also leaves it open to the Secretary of State to make further Regulations as to conditions to be met for such sharing, without indicating what those might be.

16. Further, Clause 41 says that *'arrangements'* must be in force to ensure some limited safeguards are put in place for sharing material from a targeted warrant (although only if the authorising agency considers that appropriate) – but primarily to limit the extent of any disclosure/copying of the material. There is also similar reference in clause 117 to material from bulk interception being handed over to overseas authorities, to which the clause 118 'safeguards' are said to apply. Those safeguards are again extremely limited and seem to relate only to the Secretary of State ensuring that restrictions are in place to avoid 'unauthorised disclosure' in legal proceedings (clause 42). There is simply nothing to ensure human rights violations do not occur, such as the sharing of material which may then lead to secret detention, torture, unfair trials, or other activity that would be unlawful if it occurred in the UK (and perhaps even thus to UK complicity in such activity). Where does the chain stop? Furthermore, it appears that these *'arrangements'* referred to in clauses 41 and 117, similarly to other *'arrangements'* foreseen in the draft Bill (see clauses 40 and 117), are to be entirely secret ones, hence kept away from any proper parliamentary and public scrutiny and accessibility.

17. Amnesty International UK has not been able to identify any provisions at all in the draft Bill (even as limited as those in relation to providing material to overseas authorities) dealing with the receipt by the UK of material obtained through interception by overseas partners, other than in Schedule 6. Schedule 6 provides at 2(2) a bare statement that Codes of Practice will cover the process for overseas requests and handling data received from them. Not only is this a wholly inadequate provision given the scale of what occurs, it makes no mention whatsoever of communications material received otherwise than through a specific request.

18. ***Amnesty International UK recommends that the Draft Bill be amended to provide a clear, accessible framework governing intelligence sharing that ensures, inter***

alia, it is as limited as possible for permissible purposes, and does not include receiving or sending the product of bulk surveillance or material obtained through human rights abusive methods.

<u>The authorisation process:</u> Are the proposed authorisation processes for such interception activities appropriate? Is the proposed process for authorising urgent warrants workable?

19. Amnesty International UK does not consider the proposed authorisation processes to be compatible with the UK's human rights obligations.

20. The so-called 'double-lock' process fails to ensure a proper independent authorisation process. As is reflected in judgments from both the European Court of Human Rights and the Court of Justice of the European Union, the decision as to whether to issue a warrant should be made by a judicial authority with sufficient independence from the executive[77]. Otherwise, the prior authorisation cannot provide an effective fetter on executive discretion – it is not a true safeguard against abuse. The draft Bill instead vests the power to issue an interception warrant with the Secretary of State (see, *inter alia*, clauses 14, 107). It is the Secretary of State who receives the application from the relevant body, considers its content and takes the crucial decision as to whether to issue a warrant. The Judicial Commissioner ('JC') is charged merely with approving that decision (clauses 19, 109) – a JC may only "*review the person's conclusions*".

21. That review, by virtue of clauses 19(2) and 109 (2), must be carried out on judicial review principles. Such an assessment cannot cure the defect in the allocation of decision making power in this process. If, indeed, the intent of the drafters was to give the JC the power to conduct a full merits assessment of the warrant that the Secretary of State has authorised, as has been suggested in some quarters, then there is simply no reason for this limiting provision. Clause 19(2) is thus either a restriction on the power of the JC, or unnecessary and unnecessarily complicating the question of what the role of the JC is here.

22. It does not in Amnesty International UK's view satisfy the requirement that the
> "*authorisation authority … [be] capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security. It must also ascertain whether the requested interception meets the requirement of "necessity in a democratic society", as provided by Article 8 § 2 of the Convention, including whether it is proportionate to the legitimate aims pursued, by verifying, for example whether it is possible to achieve the aims by less restrictive means*" (*Zakharov* at 260)

[77] European Court of Human Rights, *Roman Zakharov v Russia,* para 233 ; Court of Justice of the European Union, *Digital Rights Ireland* case, C-293/12, Grand Chamber, Judgement of 8 April 2014, para 62.

23. It is also unclear whether the JC will have before them the underlying warrant application that forms the subject of the Secretary of State's decision, or merely some document or other summary of her conclusions, and even if they have the warrant application, what level of evidence will be available to them. An express requirement that the JC has all the relevant information and documents, and certainly no less than what needs to be provided to the Secretary of State, is necessary.

24. Crucially, it is also of major concern that the JC is excluded from the process of accessing and examining intercepted material obtained under a bulk interception warrant in circumstances other than the ones foreseen by clause 14(2) (targeted examination warrants). There is no valid reason whatsoever for providing less safeguards with regard to the access and examination of such intercepted communications, a difference of treatment which is discriminatory

25. The modification process adds to the concerns. '*Major*' modifications which affect the conduct authorised under targeted warrants may be made under clause 26 without any involvement whatsoever of a JC. Such a modification may include adding the name of a person, organisation or set of premises (clause 26(2)) thus fundamentally altering the nature of the warrant in question without any independent involvement at all. Similarly, what are deemed by the draft Bill to be *'minor'* modifications, which nevertheless include *'adding, varying or removing any factor specified in the warrant'*, also do not involve the JC at all. As for bulk interception warrants, while the provisions for their modification prescribe that the JC must be involved in a similar way as during the original approval process when it comes to adding or varying an operational purpose, the JC is not involved when an operational purpose is removed (clause 114(6)). What happens, for instance, if a purpose is removed and the conduct authorised does change, but not commensurately with the more limited purposes of the modified warrant?

26. It is worth noting that not even the Secretary of State is necessarily involved in the process leading to certain modifications of bulk interception warrants (see clause 114(8)), or indeed to modifications of targeted warrants (see clause 26(6) and 26(11)). Furthermore, clause 114(9) does not sufficiently specify what is meant by *'a way which does not affect the conduct authorised or required by [the warrant]',* hence potentially becoming a problematic loophole in the legislation. Finally, no *'double-lock'* whatsoever is foreseen in cases of certain mutual assistance warrants (clause 28).

27. Amnesty International UK is further concerned by the requirement that JCs must give written reasons for refusing to approve the Secretary of State's decision, although not for approval. This appears to create an assumption of approval.

Secrecy – the need for a designated person to advocate for human rights during the warrant authorisation process

28. Amnesty International UK remains opposed to secret justice. While the process of authorisation of interception warrants (rather than the process of remedying of

human rights violations) can legitimately take place without knowledge and presence of the person concerned, it remains highly desirable to enhance the adversarial nature of such proceedings. This would hope to ensure all angles are covered and the human rights implications of the decision are properly and fully considered.

29. As such, there should be added to the Bill a requirement for a designated person challenging the request and advocating for the protection of human rights and fundamental freedoms. This person should be fully involved in the authorisation process, as a necessary further safeguard against abuse.

Urgent warrants

30. The urgent warrant process, in Amnesty International UK's view, is also incompatible with the UK's human rights obligations. Interestingly, *Zakharov* included a complaint that in urgent situations communications in Russia could be intercepted without judicial authorisation for up to 48 hours [para 191] - note that the draft bill offers 5 (working) days for un-approved interception, more than double what Russia's government demands. There, the Court concluded there were insufficient limits on deciding when such urgent warrants were justified and they could thus be abused. The same applies to the process in the Draft Bill.

31. It is difficult to see any limit whatsoever in clause 20 other than that the person who issued the urgent targeted warrant (who by virtue of clause 22(4) may be a senior official not the Secretary of State) considered "*that there was an urgent need*" to do so (clause 20(1)). As such, and noting that the UK judiciary are well used to dealing with urgent and complex applications out of hours, there seems little justification for the existence of this urgent process, and none at all for such a lengthy period in which the executive may operate free of any constraint whatsoever. It is easy to see how such a provision may become a loophole ripe for excess and/or abuse.

32. ***Amnesty International UK recommends that the authorisation process be amended so that (i) decisions to authorise warrants are taken by an independent judicial body following the application of (or with the interim non-statutory approval of the application by) the Secretary of State, or through a similarly full judicial authorisation process. (ii) Such a decision would require full disclosure of all relevant materials underlying the application. (iii) To the extent the decision to authorise the warrant has to be made without the knowledge and presence of the person concerned, it should also involve the participation of a designated person challenging the request and advocating for the protection of human rights and fundamental freedoms.***

<u>Oversight:</u> Are the powers sought sufficiently supervised? Will the oversight bodies be able adequately to scrutinise their operation? Would the proposed Judicial Commission have sufficient powers, resources and independence to perform its role satisfactorily? Are the appointment and accountability arrangements for Judicial Commissioners appropriate?

33. Amnesty International UK does not consider that the oversight proposals will provide sufficient independent supervision. In particular, the dual function of the small group of JCs raises independence and effectiveness concerns. They will be both a part of the surveillance process in authorising warrants, and also part of the oversight system in that JCs must review, including by inspection, the exercise by public authorities (presumably thus including themselves) of functions relating to interception of communications (clause 169 (1)).

34. In the litigation concerning investigations into allegations of article 3 abuse in Iraq carried out by the military, the UK High Court referred to the problem highlighted in relevant Strasbourg cases where investigating officers (in the instant case being part of the Royal Military Police) "*formed part of the same hierarchy with no provision for institutional or individual independence*". It concluded that while that did not apply in the circumstances of the case, the key question remained "*whether on the facts of a given case, the service police is independent of the events or personnel being investigated*"[78]. Amnesty International UK refers to this simply to highlight that this dual function of a small group of Commissioners may raise problems on the facts should serious questions arise over the appropriateness of a warrant issued in any particular case requiring proper investigation. We consider it would be preferable to separate out the authorisation and oversight functions of the judicial commissioners to avoid such difficulties arising.

35. The Secretary of State can also – by way of regulations rather than full primary legislation – modify the functions of the IPC or "*any other*" JC (clause 177). That is an extraordinarily wide power to vest in the Secretary of State and raises significant independence as well as proper process concerns. That is particularly so given it is the Secretary of State and those responsible to them who will be particularly under the scrutiny of the Commissioners and who will therefore be deeply affected by the way their functions are exercised. Amnesty International UK considers such a power should not be simply left to secondary legislation (clause 197 provides that 'Regulations' here means statutory instruments may be used) but laid in primary legislation and properly debated by Parliament.

36. Further, Amnesty International UK is concerned by the weighty conditions placed on what are supposed to be robust, independent investigations by highly experienced judicial commissioners in clauses 169 (5) and (6) of the Bill. These include a mandatory instruction to ensure a JC does not in the carrying out of their oversight functions "*jeopardise the success of an intelligence or security operation or a law enforcement operation*" or "*unduly impede the operational effectiveness of an intelligence service, a police force, a government department or Her Majesty's forces" (clause 169(6)).* That very broad drafting not only lacks the required clarity of the law for such a serious provision affecting oversight, but has the potential to jeopardise its effectiveness. An expert authority charged with investigating, *inter alia*, whether such operations and agencies are working lawfully and appropriately,

[78] *R (Ali Zaki Mousa) No.2* [2013] EWHC 1412 (Admin), [2013] HRLR 13 at 111-112

should not be constrained in such vague terms – particularly if the public are to trust in their reports.

37. For that trust, it is also necessary that oversight be as transparent as possible. As such, the wide discretion afforded to the Prime Minister (see above as to the lack of clarity in such terms as 'national security') in deciding whether or not to publish any additional oversight directions he may make to the IPC (clause 170(4)) is deeply unsatisfactory. The same concerns arise in the context of the Prime Minister's wide discretion to exclude any part of the IPC's reports from publication (clause 174).

38. The system of notification (such as it exists) is also deeply unsatisfactory. Clause 171 provides that the IPC must inform persons of any "*error",* but only in so far as the IPC and the Investigatory Powers Tribunal ('IPT') consider it is a serious error (they are banned otherwise from reporting it), and that the IPT considers it is in the public interest for the person to be so informed. However, it is difficult to understand how the IPT can properly undertake an assessment of "*the seriousness of the error and its effect on the person concerned*" [clause 171(5)] when it will not have before it any independent evidence as to that effect. It is also difficult to understand the reason why there needs to be a *joint* decision by both the IPC and the IPT before the person concerned is notified (clause 171 (2)). Moreover, it is troubling to see a specific clause (s.171(4)) instructing the assessors that a breach of an individual's ECHR rights "*is not sufficient by itself for an error to be a serious error*".

39. This falls far short, first, of the necessary requirement under international human rights law to notify all persons that they have been subjected to surveillance (and the grounds for it and materials selected, as well as potential remedies) as soon as this may be done without jeopardising the legitimate purpose of the surveillance. Not only is notification in the Draft Bill confined to an ill-defined concept of 'errors', but second, to an unnecessarily onerous test. Such requirements not only fail to meet human rights standards but are plainly biased in favour of secrecy (encouraging an approach that says secrecy should be the norm) rather than transparency wherever possible.

Are the new arrangements for the Investigatory Powers Tribunal including the possibility of appeal adequate or are further changes necessary?

40. The concerns as to the effectiveness of the oversight scheme are enhanced by Amnesty's own experience of the IPT. While we welcome the addition of a right of appeal on a point of law to the Court of Appeal, that single change does not go far enough.

41. In order to explain Amnesty International UK's particular concerns, it is necessary for this Committee to have some understanding of our experience of the IPT. The Committee will doubtless be aware that Amnesty International Ltd. (the International Secretariat) joined with several other NGOs in litigation commenced in 2013 challenging the lawfulness of the UK's Tempora regime, and of its intelligence sharing with the US in relation to the US PRISM and Upstream mass surveillance programmes.

42. With regard to the intelligence sharing issue, while the first judgment (December 2014) rejected to a large extent the arguments put forward by the claimants, the purported lawfulness of the intelligence sharing scheme was heavily predicated upon the disclosure during the litigation of a short summary (or similar – this Note was amended more than once after discrepancies were only brought to light following requests for clarification by the claimants) of the otherwise secret policies in place. A further judgment later (February 2015) declared such intelligence sharing prior to this disclosure to have been unlawful. During the proceedings, Amnesty and others raised serious concerns as to the processes of the IPT, including the holding of closed hearings to determine issues of law.

43. As regards the UK surveillance regime and practices, once the IPT decided in its December 2014 ruling that the regime was lawful, it then decided to assess the issue of proportionality in closed session. The claimants were not given the opportunity to meaningfully contribute to that assessment. That alone was of serious concern.

44. On 18 June 2015, we were then provided with a draft judgment. It declared that two of the claimant NGOs, the highly respected Legal Resources Centre ('LRC') in South Africa and the Egyptian Initiative for Personal Rights ('EIPR'), had been the victim of Article 8 violations. In respect of the both, the IPT concluded that their communications had been lawfully intercepted. However, it said that the LRC's communications while 'proportionately' selected for examination, were not so selected in accordance with GCHQ's 'internal policies'. In respect of the EIPR, it was said that their communications had been lawfully accessed, but had been retained too long in breach of internal policies (a so-called 'technical' breach). Despite having heard no submissions on the topic, it concluded that the EIPR had "*not suffered material detriment, damage or prejudice as a result of the breach*". Amnesty received only a one line ruling that the IPT had not made a determination in its favour.

45. There was no explanation of such matters as (a) the statutory purposes for which the communications were intercepted; (b) the nature or content of the internal procedures which were breached by GCHQ (for example, whether the procedures were automated or manual) and how they were breached; (c) the reasons why GCHQ's internal policies were not complied with and what procedures were supposed (but failed) to secure such compliance; (d) whether the errors were isolated mistakes or broader systemic errors which may have affected a larger class of people; (e) whether the errors had previously been identified by any internal audit, or by the Interception of Communications Commissioner, or whether the errors were only identified following these proceedings being brought in the Tribunal; (f) whether the communications that were processed in breach of Article 8 were shared with, or made available to, any other agency or department outside GCHQ. The parties were given the opportunity to correct any typographical or other errors in the judgment before it was made public, but that was all.

46. On 1 July, the IPT then wrote to the Parties notifying us that the finding in relation to EIPR in fact related to Amnesty International Ltd, a mistake which the government had failed to pick up at the corrections stage, but had now apparently identified to the judges. We wrote to the IPT, asking further questions and expressing concern as to how it was possible for the Tribunal to have made such an error as well as why it was not picked up when the government commented on the draft judgment (and requesting an Open Determination explaining this). A very limited letter of response was received on 24 July 2015, however it has still not satisfactorily been explained how such an error could be made if the IPT did indeed make an individualised, detailed analysis of the proportionality of the surveillance of each of the applicants.

47. It should also be noted that Amnesty's communications were said by the IPT to have been intercepted and accessed under what is the equivalent of the bulk interception warrants provided for in the Draft Bill. Hence the examination of these communications would supposedly have happened without objection from the Secretary of State nor, subsequently, of the oversight bodies (as well as without any identification of the procedural breach) in so far as they were aware of it. The Intelligence and Security Committee report of 2015 stressed that "[*o]nly the communications of suspected criminals or national security targets are deliberately selected for examination*" (para J, p32). As such, there was a significant onus on the IPT to explain the government's justification for selecting our communications for examination, which we did not receive. Despite parliamentary questions on both surveillance of Amnesty and whether other human rights charities have also been intercepted, Amnesty is in no better position now to understand why we were the target of surveillance than when the judgment was released.

48. It is against that background that Amnesty International UK's general concerns about the effectiveness of the IPT's oversight function should be viewed, including the holding of hearings concerning the remedy of human rights violations without proper involvement of the alleged victim. The restrictions on fair trial rights in the IPT (including the restrictions on disclosure and evidence, secrecy of proceedings and limited reasons given to claimants both successful and otherwise) are not proportionate, impair the essence of fair trial rights and have been shown to lead, *inter alia*, to errors and unfairness as predicted. It is necessary for the powers and rules of the IPT to be revisited, *inter alia*, to introduce proper openness and transparency. The existing Tribunal is not an effective oversight body.

49. ***Amnesty International UK recommends that the oversight mechanisms be revisited in their entirety to ensure proper safeguards against abuse.***

<u>Special protections:</u> Are concerns around accessing journalists', legally privileged and MPs' communications sufficiently addressed?

50. Amnesty International UK does not consider that the concerns over interception of and access to these communications are sufficiently addressed by the Bill. In particular, it is wholly inadequate to provide for protections for legally privileged

communications solely in a Code of Practice rather than in the legislation itself. Schedule 6 merely provides, as is normal with such codes, that they will be something those carrying out interception must '*have regard to'* – it does not have the same force in domestic law as legislation. Moreover, without sight of that Code, the question cannot be taken much further.

51. There is however a further category simply not covered in any way by the draft scheme, and that is protection for human rights and similar organisations. The integrity of Amnesty's communications is of paramount importance to our work. As an organisation frequently in contact with victims of human rights abuses, human rights defenders and other sources, often at risk from their own governments, and which intervenes in litigation worldwide to promote human rights, it is essential that we are able to communicate freely and confidentially if we are to fulfil our role. Where an NGO is involved in matters of public interest it has long been recognised that it is exercising a role as public watchdog of similar importance to that of the press and warrants similar protections to those afforded to the press[79].

52. For the draft bill to comply with articles 8 and 10 ECHR, it must therefore provide sufficient indication as to how NGOs in this position will have their confidential materials treated just as it does for those of other sensitive professions.

53. ***Amnesty International UK recommends that provisions for special protection for sensitive professions be included in the body of the legislation, and include human rights NGOs.***

[79] see *Guseva v Bulgaria* application no. 6987/07, 17 Feb 2015, para 38 and the cases cited.

David Anderson Q.C.—supplementary written evidence (IPB0152)

Introduction

1. Having had a (lengthy) say in my June 2015 report "A Question of Trust" (AQOT), and given oral evidence on 2 December 2015, I do not burden the Committee with reiteration of my recommendations that were not accepted, or with further submissions on the many specific issues thrown up by the draft Bill.

2. Many of the detailed concerns which I did not have a chance to raise orally (for example in relation to thematic warrants and their modification,[80] error reporting[81] and national security exemptions[82]) are covered in the impressive written submissions recently made to the Committee by IOCCO and by Tom Hickman. I have seen those submissions in draft and do not repeat them here.

3. Nor do I need to elaborate on the features of the proposed Investigatory Powers Commission[83] which I have previously advised are necessary if it is to fulfil its potential as a well-informed, independent and authoritative guarantee that some extraordinarily extensive powers are not misused. These include:

    a. the power to issue guidance, with a view to building up a consistent and so far as possible public body of principle governing the use of investigatory powers (AQOT Recommendation 95) and

    b. independent input from standing counsel, technical experts and others (AQOT Recommendation 110-111), which would be of particular value when considering whether to approve bulk warrants.

    Though neither of those features is specifically provided for in the Bill, it appears at least to be intended that the Commission will have the discretion and the funding to ensure that they can form part of its work should the Investigatory Powers Commissioner so decide.

Need for bulk powers

4. It was put to David Davis MP on 16 December (Q177) in relation to "*bulk interception, bulk acquisition of the collection of communications data and bulk equipment interference*" that I had looked at them and pronounced myself "*satisfied that those powers were necessary*". While there is much truth in that comment, I

[80] Hickman, paras 11-23; the draft Bill does not offer the protections envisaged in AQOT 14.62-14.63 and Recommendation 34.
[81] IOCCO, paras 9-11; Hickman, paras 81-88.
[82] IOCCO, para 17.
[83] Regrettably not constituted as such in the draft Bill: AQOT Recommendation 82; IOCCO, para 8, first bullet.

should like to clarify what I did and did not conclude in relation to the need for bulk powers.

5. The central point is that the appointed Commissioners and the IPT are best placed to judge whether each of these powers is necessary and proportionate. The Commissioners have the advantage of longer and more thorough exposure to the exercise of those powers than did I; and the IPT in a number of cases has had the additional advantage of detailed and formally-presented argument from both sides.

6. My own detailed briefings however left me in no doubt as to the utility of:

    a. ***bulk data collection,*** *"particularly in fighting terrorism in the years since the London bombings of 2005"* (AQOT 14.39-14.45 and Annex 9); and

    b. the ***compulsory retention by CSPs of communications data*** (AQOT 14.14-14.22, Annexes 10-14).[84]

7. Whether those powers are proportionate in law is ultimately for the courts to decide, in the light of the conditions and safeguards provided for in the Bill. The relevant decided and pending cases are set out in AQOT chapter 5 and include *Digital Rights Ireland*, to the extent that this judgment is applicable to domestic law (AQOT 5.76 and Recommendation 16). See further *Schrems* (CJEU, 6 October 2015) and the *Davis/Watson* case, on which I have written twice since AQOT.[85]

8. My report however contains no independent conclusions on the necessity for or proportionality of:

    a. the use of ***bulk personal datasets*** (AQOT 7.69-7.70), where I noted simply that the conclusions of the ISC and of the Intelligence Services Commissioner – who has been reviewing their use for several years – were consistent with the information and demonstrations I was given at all three agencies;

    b. the ***newly-avowed section 94 bulk collection power***, which I was not authorised to refer to in AQOT, on which IOCCO has not yet reported and of which I have remarked that I made no assessment of its necessity or proportionality and that the agencies "*should have to defend that power in the public space, where people can evaluate the claims they make and evaluate the risks as well as the benefits*";[86]

---

[84] Indeed the value of this power for criminal investigations has been accepted even by the CJEU, which in other respects appears wary of it: AQOT 5.67.

[85] https://terrorismlegislationreviewer.independent.gov.uk/dripa-2014-s1-declared-unlawful/ (17 July 2015); https://terrorismlegislationreviewer.independent.gov.uk/daviswatson-appeal/ (20 November 2015).

[86] https://terrorismlegislationreviewer.independent.gov.uk/the-big-reveal/ (7 November 2015). See further my answer to the Committee's Q66: "*There may be a question as to the added value of retaining possibly similar categories of data in a single place. Is this all about speed of access, or are there other advantages that the intelligence agencies glean from it?*"

c. ***internet connection records***, which have now been the subject of an operational case, but as to which much depends on deliverability (evidence of Jesper Lund) and other factors, including the mechanisms for authorising access: AQOT 14.323-14.38 and answers to QQ 64 and 74; or

d. ***bulk equipment interference*** (formerly CNE), which in view of pending IPT litigation and the limited nature of my remit (AQOT 1.10-1.11) I touched upon only briefly in my report (AQOT 6.24-6.31, 7.62-7.65).[87] The remarkable potential for this capability is evident from the Snowden allegations relating to the hacking of and implantation of malware into systems operated by persons not themselves suspected of wrongdoing: AQOT Annex 7, paras 16-18.

9. I do not intend to suggest that any of the bulk powers I have referred to are unnecessary or disproportionate in the form provided for in the Bill. Indeed I view with a degree of scepticism (because they do not square with my own observations) suggestions that such powers are persisted in despite being useless or even counter-productive in practice. My point is simply to make clear what I did and did not conclude, so that false comfort is not taken from my Report in areas where it is incumbent on the Government to justify powers that it seeks to enshrine for the first time in clear law.

10. In that respect, I endorse the advice of Jim Killock (Q127) and Eric King (Q207) that the Government should do more to make an operational case for the bulk powers that it seeks to preserve, as it has for the ICR power that it seeks to introduce. That course seems to me, indeed, to be very much in the Government's own interest:

a. It is the Government that bears the burden (including the legal burden) of demonstrating that inroads into the legal protection afforded to privacy and to personal data are necessary and proportionate – particularly where (as in the case of equipment interference) those inroads are active rather than passive, and may affect the interests of companies and individuals in friendly nations who are not themselves suspected of wrongdoing.[88]

b. Though there must by now be evidence of the utility of these powers, they have not been the subject of parliamentary debate, and each may ultimately have to be defended in European courts which – because of their limited

[87] Similarly, in relation to targeted equipment interference by the police, I noted only that "*A debate is clearly needed as to how law enforcement can best utilise CNE and what safeguards should apply*": AQOT 9.75-9.76. In the course of my own review I did not see a detailed operational case from the police on the gaps that are said to exist in their existing property interference powers, or on how the power now envisaged in clause 89 of the draft Bill might be used.

[88] The use that it has been suggested can be made of related communications data (written evidence of Graham Smith of 22 December 2015, paras 117-137, including reference to the Snowden allegations re KARMA POLICE) indicates that this is another area where more information is needed.

capacity to consider closed material – will need to be persuaded on the basis of evidence in the public domain.

c. If an evidence-based public defence of the powers is not attempted, the argument may yet be won at European level by those who – having never been exposed to the evidence – assert the powers to be either useless[89] or more sinister in their operation than is in fact the case.

11. More therefore needs to be done, in my opinion, to give effect to AQOT Recommendation 122.[90] As I said to the Committee (Q63):

> "Nobody should expect the Government to give away operational secrets or information that is damaging to national security, but it seems to me that we need more in the way of information if [bulk powers] are to be truly accessible and foreseeable."

I hope, accordingly, that the good start made by GCHQ in sanctioning the publication of the anonymised case studies in AQOT Annex 9 will be accompanied by the shedding of further light on the utility that is claimed for other bulk powers, not only in the secret environment of ISC and IPT closed hearings but, to the maximum extent possible, to Parliament and the public. To my mind, the need for widespread acceptance of these powers, including internationally, requires no less.

7 January 2016

[89] See, for example, the reports referred to at AQOT 14.44(a).

[90] "Public authorities should .. be as open as possible (cf ISC Report, Recommendation BBB). They should consider how they can better inform Parliament and the public about why they need their powers, how they interpret those powers, the broad ways in which those powers are used and why any additional capabilities might be required. They should contribute to any consultations on the new law, so as to ensure that policy-making is informed by the best evidence."

Andrews & Arnold Ltd—written evidence (DIP0001)

1st December 2015
Written evidence regarding Investigatory Powers Bill for Joint Committee.

Andrews & Arnold Ltd are a small but technical Internet Service Provider (ISP), and FireBrick Ltd are a manufacturer of routers, firewalls, call servers, VPN servers, and related equipment. I personally have extensive experience in technical and operational aspects of running an ISP for over 18 years, having written the underlying operating code of our core routers and equipment. I have previous experience in mobile telephony and landline telephones and exchange equipment.

Key points:-

- There are a number of privacy issues which cause concern, especially web logs and interference
- I feel the bill needs to clarify and limit scope of data retention order to be in line with the expectations of the Home Office and so as to minimise misuse by future governments
- I feel that the current proposed 100% cost recovery needs to be on the face of the bill
- I feel retentions orders should not be required to be secret, though operators may choose not to disclose details
- I feel that the usefulness of Internet Connection Records is over stated and misunderstood, and will also have diminishing use over time, so should be considered not cost effective now.
- There needs to be clarification on DNS traffic being “content”
- There needs to be clarification on interaction with Data Protection Act
- Attempts to ban use of end-to-end encryption are a concern

Ethical/Privacy issues

I am quite sure there are a number of issues which are better addressed by organisations such as Privacy International, Open Rights Group or similar. However there seem to me to be some clear issues with the bill as follows.

1 Web logs

The explanatory notes and discussions with the Home Office make it clear that there is an intention for retention notices to require, in some cases, the logging of the web site name visited by an operator’s customers.

Whilst telephone call data records do reveal some information about the subject it is clear that retention of details of every web site visited reveals much more about a person. It can be used to profile them and identify preferences, political views, sexual orientation, spending habits, and much more. It is also useful to criminals as it would easily confirm the bank used, and the time people leave the house, and so on.

This is plainly sensitive personal information, and it is clearly a huge invasion of privacy to collect and retain this information on innocent people.

It is also a valuable target for criminals and so a risk for operators to retain this data.

There have been arguments that this is not "mass surveillance" as nobody will look at the logs unless you are later part of some investigation. However, I am quite sure the same argument would not work if, for example, the law required a camera in every room in your house. The fact the logs may not be looked at does not mitigate the obvious invasion of privacy and mass surveillance by the very collection and retention of these logs.

As this level of logging is a new power over and above existing retention regimes, it deserves even more scrutiny. **I feel that this level of logging is unjustified and not proportionate or ethical and should be specifically excluded from the bill.**

2 Equipment Interference

Equipment Interference (or legalised hacking) is one of the most intrusive powers in the bill. It therefore seems unconscionable that "bulk equipment interference" orders are included in the bill. This could literally be placing a camera in people's homes via they PCs and phones without them knowing. Equipment Interference can also impede operation of devices, and make it easier for criminals to access devices. Surely such an intrusive power, if allowed at all, should only be targeted at the most serious of criminal suspects? **I feel that bulk equipment interference should be removed from the bill.**

It also seems that one of the means by which equipment interference can be carried out is by exploitation of a vulnerability in a computer system. Where such a vulnerability is known by the intelligence services they have a clear moral obligation to responsibly disclose that vulnerability to the manufacturer so that it can be rectified. **I feel that use of vulnerability in equipment should not be permitted, as allowing them encourages the intelligence services to keep vulnerabilities secret, thus exposing everyone to increased risk of criminal activity.**

Technical/compliance issues

Data Retention

I was pleased to have the opportunity to discuss data retention with the Home Office yesterday thanks to the Internet Service Providers Association. The discussions were interesting. The main concerns from the ISPA members present, mostly quite small ISPs, is that they could be subject to a retention notice, and that such notice could require "Deep Packet Inspection" which would have significant cost implications.

3 Scope of retained data

It seems clear from the Home Office that they are intending to only serve notices on those larger ISPs that are already subject to notices, and with which they have already had extensive discussions. They have indicated that they are not intending to target smaller ISPs,

and even if they did, that ISPs would not be expected to log and retain data for which they simply do not have such a capability, and that they would not expect any collection of "third party data" or information from "over the top services". However, the bill, as worded, does not embody these intentions. **We would like so see specific caveats in part 4. Specifically:-**

- 71(9) should make clear that data is only that which *"is generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication (whether or not a person)"*. This wording is from the definition of an "internet connection record" in 47(6) so clearly part of the intended description.
- That is made clear by a definition that "process" in this context means that the operator considers the data and takes some decision on it (such as routing packets) and not simply that the data passes through the ISPs network.
- 71 should also contain a restriction that it must be "reasonably practicable for the operator to collect and retain the data".

None of these changes should impact the intentions of the Home Office. It would still allow the key aspects of logging that seem to be the intention of the Home Office:-

- An email provider to log email addresses as these are processed and logged.
- A telephony provider to log call records.
- A mobile operator to log SMS messages.
- An operator that uses a "web proxy" to log web site names visited.
- An operator that uses Carrier Grade NAT (CGNAT) to log NAT sessions (connections).

It would, however, limit the scope of future governments to expand the retention beyond current intentions without a change to the legislation. The wording chosen also fits in with the cost implications of the bill as they relate to the activities which would significantly increase costs for the ISP such as Deep Packet Inspection (DPI).

4 Use of the term "Internet Connection Record"

The explanatory notes, and one of the clauses in the bill, make use of the term "Internet Connection Record". We are concerned that this creates the impression that an "Internet Connection Record" is a real thing, like a "Call Data Record" in telephony.

An ICR does not exist - it is not a real thing in the Internet. At best it may be the collection of, or subset of, communications data that is retained by an operator subject to a retention order which has determined on a case by case basis what data the operator shall retain. It will not be the same for all operators and could be very different indeed.

We would like to see the term removed, or at least the vague and nondescript nature of the term made very clear in the bill and explanatory notes.

5 Gagging

77(2) prohibits an operator for revealing the existence or content of a retention order. Whilst I can understand operation reasons for not revealing targeted intercept warrants, a retention order does not relate to a suspect or a case, and so has no reason to be secret.

The Home Office were quick to confirm that this clause is at the request of the larger operators with which they have had discussions, and whom do not wish to reveal the existence of notices.

This makes no sense. If an operator wants to keep a notice secret they can simply do so. If an operator wants to discuss the notice with equipment vendors, technical working groups and forums with other ISPs or even their customers they are prohibited from doing so. Also, this clause only prohibits the operator disclosing the notice, and does not prohibit the Secretary of State, the Home Office, the Investigatory Powers Commissioner or anyone else who may know of the order from doing so, and so it does not even meet the requirement of the larger operators.

This clause simply needs removing.

6 Cost recovery

The Home Office also indicated that, as now, that operators would receive 100% cost recovery.

It is worth noting that this bill is not an attempt to regulate telecommunications operators because they are operating business models that are offensive to society or otherwise engaged in activity that needs controlling! This bill is specifically to force operators to provide a service to the authorities to help with criminal investigations of other parties, where the telecommunications operator is not themselves in any way complicit or liable. It is clear, therefore, that the operator should receive at least 100% cost recovery for providing this service - indeed, for most services provided a company would expect to be able to make a profit.

As this is the current intention it seems sensible that the face of the bill should state clearly that at least 100% cost recovery applies, and not the current wording which simply guarantees that it is not actually “nil”. There can surely be no objection unless the Home Office are planning to stitch up operators in future.

We would like to see the bill specifically state that at least 100% cost recovery applies.

7 DNS logs

It is not clear if there would be any logging of DNS requests. I specifically asked the Home Office if, under traditional call logging, the content of a call to Directory Enquiries would be recorded and logged by the operator. It seems not, and this seems to make clear that the content of such a call is “content” and not “communications data”. As DNS is the equivalent service to Directory Enquiries for Internet Access, I feel that the definitions should make clear that DNS lookups, or indeed any form database access lookup, is to be considered

content and not communications data. The communications data in such cases being simply that a connection (request/reply) was made to a DNS server and who made it - not the content of what was looked up.

We would like to see clear wording to exclude the content of a DNS request ,or other database query, from "communications data", and clearly define it as "content".

8 Justification for "Internet connection records"
In the briefing with the Home Office the bill was explained, and we heard a story very similar to Theresa May's comments along the lines of:-

"Consider the case of a teenage girl going missing. At present we can ask her mobile provider for call records before she went missing which could be invaluable to finding her. But for Internet access, all we get is that the Internet was accessed 300 times. What would be useful would be to know she accessed twitter just before she went missing in the same way as we could see she make a phone call"

Now, I am sure this is a well practiced speech, used many times before. I am sure the response has been nodding of heads and agreement with how important "Internet connection records" are, obviously.

However, in yesterday's meeting I, and other ISPA members immediately pointed out the huge flaw in this argument. If the mobile provider was even able to tell that she had used twitter at all (which is not as easy as it sounds), it would show that the phone had been connected to twitter 24 hours a day, and probably Facebook as well. This is because the very nature of messaging and social media applications is that they stay connected so that they can quickly alert you to messages, calls, or amusing cat videos, without any delay.

It should be noted that it is quite valid for a "connection" of some sort to last a long time. The main protocol used (TCP) can happily have connections for hours, days, months or even years. Some protocols such as SCTP, and MOSH are designed to keep a single connection active indefinitely even with changes to IP addresses at each end and changing the means of connection (mobile, wifi, etc). Given the increasing use of permanent connections on mobile devices, it is easy to see how more and more applications will use such protocols to stay connected - making one "internet connection record" which could even have passed the 12 month time limit by the time it is logged.

Connections are also typically encrypted and have some data passing all the time, so it would not be practical for an ISP, even using deep packet inspection, to indicate that the girl "accessed twitter" right before she vanished, or even at all (just that there is a twitter app on the phone and logged in).

It seems that even this emotive example is seriously flawed, and any arguments involving serious crimes unravel very quickly with the utter simplicity of using Tor, VPNs and secure messaging applications on devices these days. Yes, there are some stupid criminals, but it is getting harder to avoid using such services even without thinking about is as applications

are increasingly moving to secure service provision so as to avoid threat from criminals. It has the side effect of also hiding from law enforcement.

Given that the examples given are already somewhat flawed, I feel the whole justification for trying to log "internet connection records" at all needs to be seriously reconsidered.

9 Use of web proxies
It seems that one of the main sources of Internet Connection Records, i.e. those which provide web site names, are likely to be from operators that use a web proxy. This is the case with many mobile providers. A web proxy was a useful tool in the days of dial-up Internet and slow connections in to the Internet - it provided a faster access for web sites and reduced transit costs. Mobile operators still use them to some extent, and some even rescale images to load faster on mobile devices.

However, with the advent of 4G and faster networking they are not only becoming obsolete, but actually a costly inconvenience. As such, it seems highly likely that operators will phase these out and hence stop providing this level of logging.

Again, this calls in to question the whole justification for logging "internet connection records".

10 Carrier Grade NAT logs
Another obvious source of Internet Connection Records is the Carrier Grade NAT (Network Address Translation) boxes that are very common in mobile providers and starting to be used by some of the larger operators.

Basically these boxes allow for the sharing of IP addresses. As IP version 4 has run out, this is becoming necessary in many larger networks. They have the side effect that they may log many types of "session" or "connection" made across the network, and these logs can be retained as an "internet connection record".

Whilst this does not offer web site names, it does provide IP addresses, and could perhaps be used to find that a phone has been connected to twitter 24 hours a day, for example.

However, CGNAT is relatively expensive, and deployment of IP version 6 makes it obsolete. With major services like google and Facebook already using IPv6, it will soon be the case that this source of connection logs will also disappear.

Again, this calls in to question the whole justification for logging "internet connection records".

11 Use of https
There is also an increasing trend within the industry to encrypt everything. Once confined to on-line banking, secure web sites are now being used for normal everyday business web pages. https is already extensively used by Facebook and google and many others, and over the next few years it is likely to become quite rare for a web site to be unencrypted.

At present some level of deep packet inspection can find the web site name of an encrypted web site from the initial negotiation, but this loophole is being plugged in the more modern protocols.

Again, this calls in to question the whole justification for logging "internet connection records".

12 The future of data retention
It seems clear that the retention of any sort of "Internet connection record" is of very limited use at present. The current proponents of this logging do not understand how the Internet works. Experience of Denmark for 10 years suggests that it is not useful. It is also clear that over time the availability of such logs and usefulness of the logs will diminish.

I feel that retaining data on web page and Internet services access is therefore not viable in the long term, of limited use now, and not proportionate in terms of costs or privacy, so should be excluded from the bill.

In the long term I suspect that even call data records for telephone calls will become useless as people use more messaging applications and secure voice and video calling.

13 Data Protection
It is not clear if retained data is subject to a Data Protection Act Subject Access request, or related requests to correct such data.

This needs clarifying.

14 Encryption
189(4)(c) is a concern as it appears to effectively ban a provider from offering a service that has proper end-to-end encryption. As the government have acknowledged on many occasions, encryption is important, and any service offered must have the trust of its users. If it is possible for a service provider to even be capable of removing encryption from there service, let alone that they may be compelled to do so, then that undermines the trust in the service.

It is worth noting that there will always be way to encrypt data end to end, whether using pen and paper dice (which is simple to make a totally uncrackable encrypted message, see https://youtu.be/3G8dPAdmyss), or using popular open source software. Criminals will be capable of using end-to-end encryption that a communications provider cannot break.

However, it remains convenient for users to use service providers that offer such services, like iTunes offer iMessage, which have end-to-end encryption. Such services can be, and are, easily hosted outside of the UK. It is also possible for such services to have software provision and service provision as distinct functions (separate companies), where the communications provider cannot decrypt the message (they are not the operator that applied the protection, so cannot be ordered to remove it) and the software provider is not subject to RIPA or the new bill (as they are not a communications provider). Again, this

makes it possible to totally bypass these flawed requirements in the bill by the companies wanting to provide end-to-end encryption.

The big issue here is that if providers refrain from using end-to-end encryption for fear of such an order, or if they build in capabilities to remove encryption, then the users of such services will not be as safe from the very real threats of cyber crimes. The other issue is that such laws cannot fail to drive software and service providers out of the UK for such services, as anyone in the UK will simply not be trusted to offer an end-to-end encryption services.

Any requirements which aim to undermine provision of encryption services should be removed from the bill.

2 December 2015

Andrews & Arnold Ltd—supplementary written evidence (IPB0028)

Internet Connection Records

This document is submitted as additional written evidence following oral evidence given on 9th Dec. The purpose it to try and clarify the meaning of “Internet Connection Records” and provide an easy to understand technical background on the challenges facing any communications provider in creating and retaining such records. I appreciate the members time in reading this document.

Adrian Kennard

---

1. History

Once upon a time telephone companies were the only real providers of any sort of electronic communications, and the “telephone call” was the basic building block of that service. The telephone companies did not originally have any sort of logs of telephone calls made, but as telephone exchange equipment become more sophisticated they were able to create itemised telephone bills by recording the details of each call made. These logs are called CDRs (Call Data Records).

The concept of a telephone call is very simple, and the idea of a CDR is simple too. There are some possible complications with diverted calls and three way calls, but even so, the basic log of what number made a call to what number is easy to understand. Logs can also include calls that are being received at a “line”, and can even include calls that were not actually answered.

Obviously police access to such records was invaluable in helping criminal investigations. Eventually this became part of RIPA and the Data Retention Directive and then DRIPA.

It is worth bearing in mind that this started to happen before much was considered on Data Protection or privacy, and if such logging was being introduced now it would no doubt be a major concern for privacy groups.

With the advent of GSM and digital mobile phones, the logging was extended to include text messages.

With the advert of Internet email, the logging was extended to include emails. It is worth noting that email logs are not normally necessary for commercial reasons as there is usually no per-email charge, so this is the point at which the logging became more of a specific service to assist law enforcement rather than simply having access to what data was already there for commercial or operational reasons.

Whilst emails are not quite as simple as telephone calls, they are a relatively simple concept in terms of logging - with an email having a sender, and one or more recipients which can be logged.

Both emails and telephone calls are pretty tangible as a single "communication", with a start and an end, and a content and addressing for that communication identifying the parties involved. Text messages are, however, an example where this breaks down a little - a logical "communication" may be an ongoing exchange of many messages making for a conversation over a long period.

2. Over the top services

The Internet has become popular with some key services, indeed, some people talk of "the Web" and "the Internet" interchangeably because "web pages" were seen very much as the only thing that the Internet does (apart from, perhaps, email). Many of the more innovative features of modern communications can seem to boil down to "web pages" in that one can access Facebook, and Twitter, and email via "web pages".

In light of this, the notion of simply logging web page accesses seems a relatively simple concept, and it is easy to see how this is seen as a logical extension of the call, text and email logging of the previous data retention regimes.

Accessing a web page is also seen as a pretty clear cut "communication", again with a time, and a person involved and an address of a web site where content is fetched or viewed.

However, the problem is that this is not actually how the Internet works.

Even logging of emails is only sensibly done at a point where an "email service" is handled. There are bits of equipment that provide "email" and these bits of equipment make use of the underlying "Internet" connectivity to do so. It is crucial that previous regulations referred to "generated or processed" in terms of logging data, as email is only processed at an "email server" and not in the interconnecting Internet Service Providers. It used to be common for an Internet Service Provider to also provide the email services, but that is much less so these days.

Email is what is called an "over the top" service. It means that email is a service that exists on top of other means of communications, like Internet access. You can log an "over the top" service where there is some service provider who has some processing function such as an "email server".

As an analogy, in the telephone world, an "over the top service" might be something like "pizza ordering". You would not expect the phone company to log what pizzas people order (by listening in to they calls) even if that is technically possible, but you might expect every pizza company to log orders that are placed if that had some benefit to law enforcement. The location of the logging relates to the service you are logging.

3. Building blocks

Looking back at telephone service, there is a building block to that service which is the "telephone call" itself. Telephone calls are logged for commercial and operational reasons.

However, the Internet does not work at that level. Even the idea of a "connection" of some sort, such as a "connection to a web site" is an "over the top service" created by the equipment at each end. The underlying "Internet service" uses something called "packets". Each packet has a destination address (called an Internet Protocol, or IP, address) which works much like a telephone number to identify where the packet is to go.

However, each packet is not really a "communication" in a meaningful sense - it is some small fraction of a communication. The Internet service providers do not work in large chunks like a "telephone call" they work in these small "packets". It is even possible for some packets to go via one Internet provider and some go via another in the same logical "communication".

Also, unlike phone calls, there are a lot of these packets - seriously a lot. Even as a small ISP we may pass on literally billions of these packets every minute, and larger ISPs move colossal amounts of data. There is no built in logging of these for commercial reasons - there is no charge based on what the packets are and where they are going. At best, some totals for overall volume of data to/from each customer is recorded. The equipment to make the packets move towards their destination (called a "router") is carefully engineered to just look at the destination address of each packet and move that packet one step closer to its destination. This is often done in very fast, expensive, and optimised computer hardware that is designed to do that one job very fast. The packets are not even "looked at" by a "computer program" as such as that would take too long.

Some equipment does have some built in ability to collect some basic statistics, and using such equipment it may be possible to get some logs of some "logical connections" or "flows" that are made - where lots of packets with the same IP addresses are being sent. However not all equipment has this capability, and equipment that does may not be able to record everything in detail.

---

4. Logging web pages

The only logical place to log web page accesses is either at the web browser (the browser history), or at the web server (web access logs). The place that does not make any sense to log web pages is in the Internet Service Provider. This is because, like any "over the top" service, the browser and computer breaks down what it is doing in to packets of data, and sends these over the Internet. The final web server reassembles all of the pieces and accesses the web page in question.

The same is true for logging emails - the sending machine (PC), the email server in the middle, and the receiving machine all see an intact email, and could log it. The ISP sees just lots of small packets in-between. This is why emails are logged at an "email server".

It is a bit like saying that the postal service have to log letters sent, but they are thwarted by the fact that every sender puts the letter through a shredder first and each shredded bit of each letter is being delivered, mixed in with every other letter, to a destination where it is glued back together.

I appreciate that this sounds crazy - but really, that is how the Internet actually works. **If you want to log anything, you really need to log it where the communication is intact**.

5. Beyond "the web"

However, having explained a bit about web pages and email, even if you can log at web servers and email servers, the Internet is changing massively.

Smart phones are the key here, and are used by everyone. Unlike conventional PCs which may only have a web browser and an email client, smart phones have "apps" (application programmes). These talk to services over the Internet.

When a web browser communications with a web site, or an email client communications with an email server, it follows a well documented standard. If you picked up all of the shredded paper (the packets) and reassembled it, you could make sense of what was going on, technically, with a lot of work (and cost).

However, when a smart phone "app" communications with a server, it does not have to follow any such standard. It simply has to be something understood by both ends. So there is no way to know what is going on. Each app can be, and is, different.

They also do not communicate in small busts like "sending an email" or "accessing a web site", but instead they keep a connection (or many connections) open all of the time - especially social media and messaging apps. That one, on-going connection, can logically be involved in lots of different "communications" with lots of people, none of which is "seen" by the ISP. Much like logging email at a mail server, the only sensible place to log "social media" is at the "social media company", not the ISP.

Even when you ignore mobile phones you have to consider "games consoles" which again do not follow standards and just need both ends to understand what is communicated. That is a massive area where people can "communicate" in-game. Again, meaningful logging at the ISP is mostly impossible.

Unfortunately, with any "over the top" service, the provider may not be in the UK and subject to UK law, making logging even harder.

But it gets worse - we now see "the Internet of Things" becoming more and more of a reality with the rise of smart phones and intelligent devices, smart thermostats, smart fridges, all sorts of things in people's homes. This means that more and more of the communication that you see is not a matter of "a person accessing a service". It means that there is a hell of a lot more "chatter" going on from devices, all of the time.

6. Encryption

There is one more complication. I have likened the way the Internet works to shredding the letter you are sending, and sending all of the bits of paper from the shredder separately. This is quite a good analogy as you can see that, with a lot of work, you could put the bits of

paper back together and see what is going on. After all, the far end does so. It is very much like the bits of paper are each addressed and numbered to make that a bit easier.

However, encryption is essential to maintaining privacy and security, and this means you cannot see what is on the bits of paper any more. Yes, the addressing is there, but nothing else.

This means that any attempt to create any sort of logs of what is going on with an "over the top" service is thwarted. You cannot see in to the messages being passed to understand what is happening. At best you can see the sender and recipient of those packets of data.

Even the final addressing can be misleading as there are many services that re-route traffic (VPN and Tor and others) to hide the real source and destination of the packets. Even where you can see the destination it can simply be some common "over the top" service like iMessage which gives no clue to the real "communication" that is going on using that service, and the service provider will not see "inside" the messages if they are doing it right.

To make matters even worse a lot of services make use of "content delivery networks". These are separate service providers that specialise in delivery of data all around the world. If you see the addresses of packets going to/from one of these you have no real clue what is being communicated as the same content delivery network can be hosting data for NASA or BBC or Facebook, or even a terrorist organisation (though CDNs are unlikely to do so knowingly).

On the matter of encryption, and I cannot stress this enough, **the battle against encryption is a lost cause**. You cannot ban encryption or force encryption to have a back door, side door, golden key, escrow key, or weak link. Encryption exists - it is not a secret! It is possible to encrypt a message with no more than pen and paper and dice such that it can never be decoded by a third party without the keys, no matter how much time or computing power they have. It is possible send encrypted communications that are hidden in other data (like images and video) so that there is no way to tell there is a secret message, so even making encryption illegal does not help. Any attempt to reduce the effectiveness of encryption will ultimately have no impact on criminals, even if you make it illegal (they are criminals, remember), but will have an impact on the legitimate use of encryption by normal citizens and businesses. You can never have a back door that is only available with a court order - **mathematics does not understand court orders**, and any sort of back door makes the communications vulnerable to attack by criminals. Please, give up on all attempts to impede encryption. **Embrace encryption** as a crucial tool for security, privacy and the economy. Encourage encryption, and digital identities, and value the benefits that this brings to society. Find other ways to understand what criminals are saying (getting data at the end points or infiltrating the criminal communities and getting inside their networks).

---

7. Self service

I have mentioned logging phone calls and emails, and that you log those at the point the service is provided as an "over the top" service. Even phone calls over the Internet, whilst almost impossible to log when looking at the packets of data, can be logged at the "telephone service provider". The same is true for emails, even where the links to email

servers are routinely encrypted, the addressing of the email can be logged at the “email servers”.

There is, however, an increasing trend for applications and services to exist which do not rely on a “service provider”. It is, for example, possible to call me using a “number” which, if you have suitable phone, connects directly to my equipment under my control, and there is no “telephone service provider” to see the call, or log that it happened. The same can easily be done with emails where end users can operate their own email servers.

Whilst running your own email or telephone server is more rare, at the moment, applications on phones are more and more working directly, end to end, by themselves without relying on an intermediate service provider. The use of an intermediate service provider is seen as a weakness and point for criminals to attack. They also use encryption end to end. This means that the only logging that could be done is of the packets of data with no visibility in to that data at all and very likely no idea of what application is being used, even.

---

8. What does the Draft Investigatory Powers Bill say?

"Internet Connection Record" is not a defined thing - in the bill or in industry!

In the oral evidence session David Hanson MP seemed adamant that an "Internet Connection Record" was "defined in the bill". He referred to page 25 and asked us to work out costs based on that definition. Page 25 is in the "explanatory notes" and not the bill, and itself is massively unclear. It basically says "*It is a record of the services that they have connected to*".

I fully understand that to someone not technical, saying "*It is a record of the services that they have connected to*" seems reasonably clear. Sadly it really is not, and if you look at the actual wording of the bill, and not just the explanatory notes, it is less clear still. Remember, all an ISP sees is “packets” - those shredded bits of communications passing through the network. I hope much of the above explanation makes that more obvious.

Unlike a telephone call, or even just sending an email, even the definition of the term "connected" is complicated, as is defining the term "service". Actually what happens is packets of data are sent between devices, and as an ISP we send those packets on towards their destination. We don't "see" any sort of "connection" or "service", all was see is “packets”. The idea of “connection” is abstract and defined by the end devices.

Ideally what this means is that web sites log any access, and email servers log any emails, and telephone servers log any telephone calls. Each is an “over the top service” and not something the ISP tries to “|og” or “retain”. This is where such logging makes sense and is comparatively simple - though the concerns over storing such data securely still exist. The problem here is that many of these services are not in the UK. If you expect a foreign web site to log web accesses for you and provide data to the UK, they would expect to also provide to any other government too, such as US, or France, or China, or North Korea or Syria. I think most providers are less than keen to do that.

One possible meaning could be that we log the destination IP address of each packet. Sadly this is neither easy nor cheap as there are literally billions of such packets whizzing through our network every minute, and we are a small ISP. I do not see that being useful to law enforcement in any way. Remember may IP addresses are not the real final destination or may be some content delivery network shared by many services.

There is a protocol for a type of "connection" used in the Internet, called TCP. This is only one of many types of connection that can be made but is the most common and is used by email and web pages. It is a standard, which helps a little. So the meaning could be to log each such logical TCP connection. This would mean making something of a jigsaw puzzle of the meta data (the destination and source addresses) in each of those billions of packets as they pass and tracking millions of simultaneous logical "connections" that are happening at any one time, then logging these. Again, this is neither easy nor cheap, and even more work than above. There are also many types of "connection" - an "Internet phone call" using a protocol calls SIP does not normally even use TCP but a "connectionless" protocol called UDP, so somehow that would need to be tracked and logged too. There is no rule that applications have to use these common protocols such as TCP and UDP either, they can make stuff up and use what they like as long as both ends understand it.

Of course, it could be that what we must log is more a matter of logging each "web page" accessed with the name of the web site, and similarly for other “services" that are not actually “web pages”. Indeed, some comments made by the Secretary of State suggested this may be what was meant. This means not only the jigsaw puzzle to construct those TCP connections, but actually looking in to the data that passes on those connections, connecting the data from many packets together, and looking for a part of the information sent called a Host: header. This is yet more complexity and work and cost. Again, web pages are just one type of communication that uses a "connection". There are many other types of "connection" that could be made, and new types will come along every day or even every few hours as new applications are developed and new innovations made. Each of these is not published - we know how "web pages" work because they follow a published standard, but mobile phone apps do not have to follow any such standard, they do not even have to use TCP to communicate. So we'd have to constantly research each and every new application and protocol that people invent anywhere in the world, work out what part of that data counts as "Relevant Communications Data" and record it in some format that the police know to ask for and understand. We would not have the help of the developers in this. **Indeed, we'd have to buy and test every app ever published and reverse engineer it to work out what to log.** That would be a huge on-going undertaking at huge cost, made massively worse by the fact that each ISP is on their own not allowed to tell anyone else what they are doing with data retention.

As worded the bill does not define what is to be logged, and nothing stops an order to log and retain “all relevant communications data” with no details being imposed on all ISPs, schools, offices, or even home networks.

So the meaning of recording "what services you connect to" is really very very unclear, and the cost involved in making such logs is not something one can sensibly estimate without actual details.

9. Future

The ways that these things work is constantly changing, with new trends in technology, changes in usage by real people and devices, and innovation. This can only mean less useful information and more noise and useless data over time.

Whilst some information is still likely to be obtainable, it is obtainable only in certain places - such as email addresses logged at the mail servers. Trying to extract information from packets of data as they pass through an ISP is pretty futile now, and will become more so over time.

It makes sense for service providers to try and keep some logs and try and help law enforcement where it is proportionate to do so considering costs and privacy. Indeed, one would hope that the likes of Facebook would be keen to help with any serious criminal investigation. Over the top service provides is an obvious target for logging and retention, up to the point that they can - but any sensible provider has end to end encryption and no logging for good security reasons.

ISPs will have some operational data, and will more than likely be able to trace an IP address to a customer for a short period of time - this is often needed in some way for operational reasons, and for some ISPs with “fixed IP addresses” it will be easy to do so. The new protocol - IP version 6 - will help with this, but still not track an address to an individual device at a premises.

Sadly, even normal phone calls and text messaging and emailing, for which logging is comparatively simple, are disappearing and making way for social media and new ways to communicate. Trying to log these new services in the ISP is increasingly pointless - they need logging at the service providers, where that is possible, if the (non UK) service provider co-operates.

Whilst this is a shame for law enforcement, and forces more reliance on “traditional police enquiries”, the increasing trends in use of social media and freely sharing information with friends should help those traditional methods find leads - especially when considering examples like a missing child as often touted as a reason for needing data retention at all.

Indeed, simple cases like a missing child - if the phone is on - it is way simpler for the parent to use an app like “Find my iPhone” on Apple with family sharing to locate the child’s phone within meters than for police to make a RIPA request to a mobile operator (with much less accuracy and taking much longer). People are more and more sharing personal data in smaller family and friend groups (as well as publicly) and this hopefully makes life easier for law enforcement not harder!

10. Helping define the data types

I repeat my offer to assist in defining clear data types if that would help clarify the bill. I feel it is crucial to clearly define what is to be logged and by which parties and in what context.

I would also be happy to try and provide more technical training on how the Internet works to members if that would be of use, but I recognise the extremely limited time available to the committee to consider this bill.

I hope this submission has been useful, and welcome any questions or requests for clarification.

17 December 2015

Apple Inc. and Apple Distribution International—written evidence (IPB0093)

1. The world today faces security threats from criminals and terrorists who threaten our shared commitment to a peaceful and productive future. Apple has a long history of cooperating with the UK government on a wide range of important issues, and in that tradition, thanks the Committee for the opportunity to share our views on this topic.

2. Apple is deeply committed to protecting public safety and shares the Government's determination to combat terrorism and other violent crimes. Strong encryption is vital to protecting innocent people from malicious actors. While the Government has said it does not intend to weaken encryption, its representatives have made clear if, "the Secretary of State and a judicial commissioner think there is necessity and proportionality in order to be able to provide that information, those companies should be required to provide that information in the clear."

3. The fact is to comply with the Government's proposal, the personal data of millions of law-abiding citizens would be less secure.

Summary

4. Hundreds of millions of people depend on Apple's products and services. Our customers trust Apple and their Apple devices with some of their most personal information — their financial data, health data, family photos, videos and messages.

5. Two things have changed in a short period of time: 1) the amount of sensitive information innocent individuals put on their devices; and 2) the sophistication and determination of malicious cyber-attackers. Governments, businesses, and individuals have all been victims, and we've all been surprised by the successful implementation of exploits the experts viewed as still merely theoretical.

6. Increasingly sophisticated hacking schemes and cyber-attacks have become the new normal as individuals live more of their lives on their devices and online. Without strong defense, these attacks have the potential to impose chaos, and threaten our way of life, economic stability and infrastructure.

7. We owe it to our customers to protect their personal data to the best of our ability. Increasingly stronger — not weaker — encryption is the best way to protect against these threats.

8. The bill threatens to hurt law-abiding citizens in its effort to combat the few bad actors who have a variety of ways to carry out their attacks. The creation of backdoors and intercept capabilities would weaken the protections built into Apple products and endanger all our customers. A key left under the doormat would not just be there for the good guys. The bad guys would find it too.

9. Encryption today is as ubiquitous as computing itself and we are all the better for it. There are hundreds of products that use encryption to protect user data, many of them open-source and beyond the regulation of any one government. By mandating weakened encryption in Apple products, this bill will put law-abiding citizens at risk, not the criminals, hackers and terrorists who will continue having access to encryption.

10. Some would portray this as an all-or-nothing proposition for law enforcement. Nothing could be further from the truth. Law enforcement today has access to more data — data which they can use to prevent terrorist attacks, solve crimes and help bring perpetrators to justice — than ever before in the history of our world.

11. If the UK Government forces these capabilities, there's no assurance they will not be imposed in other places where protections are absent.

12. On the pages that follow, our submission will also take exception to the fact the bill would attempt to force non-UK companies to take actions that violate the laws of their home countries. This would immobilize substantial portions of the tech sector and spark serious international conflicts. It would also likely be the catalyst for other countries to enact similar laws, paralyzing multinational corporations under the weight of what could be dozens or hundreds of contradictory country-specific laws.

13. Finally, the bill would also force companies to expend considerable resources hacking their own systems at the Government's direction. This mandate would require Apple to alter the design of our systems and could endanger the privacy and security of users in the UK and elsewhere.

14. We are committed to doing everything in our power to create a safer and more secure world for our customers. But it is our belief this world cannot come by sacrificing personal security.

Encryption

15. Every day, over a trillion transactions occur safely over the Internet as a result of encrypted communications. These range from online banking and credit card transactions to the exchange of healthcare records, ideas that will change the world for the better, and communications between loved ones. Governments like the United States fund sophisticated encryption technology including some of the best end-to-end encryption apps. Encryption, in short, *protects people.*

16. Protecting our customers and earning their trust is fundamental to our business model. At Apple, we've been providing customers easy ways to protect their data with strong encryption in our products and services for well over 10 years. In 2003, we launched FileVault to protect data on a user's Mac. In 2010, with iOS 4, we began to encrypt data on iOS devices to keys derived from a user's passcode. We launched FaceTime in 2010 and iMessage in 2011, both with end-to-end encryption. As users increasingly entrust Apple and their devices with sensitive information, we will continue to deploy strong encryption methods because we firmly believe they're in our customers' best interests, and ultimately

in the best interests of humanity. Our job is to constantly stay 10 steps ahead of the bad guys.

17. Some have asserted that, given the expertise of technology companies, they should be able to construct a system that keeps the data of nearly all users secure but still allows the data of very few users to be read covertly when a proper warrant is served. But the Government does not know in advance which individuals will become targets of investigation, so the encryption system necessarily would need to be compromised for everyone.

18. The best minds in the world cannot rewrite the laws of mathematics. Any process that weakens the mathematical models that protect user data will by extension weaken the protection. And recent history is littered with cases of attackers successfully implementing exploits that nearly all experts either remained unaware of or viewed as merely theoretical. Every day that companies hold the ability to decrypt their customers' data is more time criminals have to gain that ability. All the while, hacking technology grows more sophisticated. What might have been adequate security for customers two years ago no longer is and that's why we've strengthened our encryption protections.

19. Strong encryption does not eliminate Apple's ability to give law enforcement metadata or other categories of data, as outlined in our Law Enforcement Guidelines. The information Apple and other companies provide helps catch criminals and save lives. It is for this reason that UK law enforcement still requests this data from us routinely. Information about our assistance can be found at http://www.apple.com/privacy/government-information-requests/

20. We believe it would be wrong to weaken security for hundreds of millions of law-abiding customers so that it will also be weaker for the very few who pose a threat. In this rapidly-evolving cyber-threat environment, companies should remain free to implement strong encryption to protect customers.

Extraterritoriality

21. Apple has been established in Europe for more than 35 years. With the exception of certain limited retail and human resources data, Apple is not established in the UK.

22. Under European data protection law, Apple Distribution International established in Cork, Ireland and iTunes S.à.r.l. established in Luxembourg have data controller responsibility for Apple and iTunes user personal data of users located in the EEA and Switzerland.

23. We take this responsibility very seriously and face sanction from data protection authorities and/or user litigation if we fail to meet those requirements. Additionally, user content is stored in the United States, and US law controls access to that data by law enforcement. Failure on the part of any relevant US entity to follow those requirements gives rise to criminal and civil liability. Most relevant, Title III of the US Omnibus Crime

Control and Safe Streets Act would subject Apple to criminal sanctions for any unauthorized interception of content in transit.

24. As defined in relevant EU Telecommunications Law, Apple is not an electronic communications service provider. The Investigatory Powers Bill seeks to extend definitions in this area to an extent beyond that provided for in relevant EU law.

25. The draft bill makes explicit its reach beyond UK borders to, in effect, any service provider with a connection to UK consumers. In short, we believe this will lead to major issues for businesses and could ultimately put UK users at greater risk.

26. The first problem with asserting such extraterritorial powers is that there will remain a proportion of service providers which will never assist British law enforcement regardless of threatened sanction because they are underground or in jurisdictions unfriendly to British interests. It is to these providers that dangerous people will gravitate.

27. Even leaving that aside, the implications for companies such as Apple who do assist law enforcement will be profound. As well as complying with local law in the countries where we are established for the provision of our services, we will have to attempt to overlay compliance with UK law. On their face, those laws would not be in harmony. Further, we know that the IP bill process is being watched closely by other countries. If the UK asserts jurisdiction over Irish or American businesses, other states will too.

28. Those businesses affected will have to cope with a set of overlapping foreign and domestic laws. When these laws inevitably conflict, the businesses will be left having to arbitrate between them, knowing that in doing so they might risk sanctions. That is an unreasonable position to be placed in.

29. The Government has partly addressed this by providing a defense for businesses who cannot comply with a warrant because of local laws (although not in all parts of the bill - see below). However, once a third jurisdiction is overlaid (home country, UK and one other), the situation soon becomes very difficult for businesses to negotiate.

30. This will not just be an issue for companies like Apple: any British business with customers overseas might be faced with having to comply with a warrant from a foreign jurisdiction which poses it ethical problems, or impinges on the privacy of British consumers.

31. Clearly this situation could arise regardless of whatever legislation is passed in the UK. But Parliament will be leading the way with this bill and needs to carefully consider the precedent it sets.

Equipment Interference

32. We believe the UK is the first national Government to attempt to provide a legislative basis for equipment interference. Consumer trust in the public and private sectors can benefit from a more concrete understanding of the framework in which these activities can take place. However, it could at the same time be undermined by a blurring of the

boundaries of responsibilities, and the bill as it stands seems to threaten to extend responsibility for hacking from Government to the private sector.

33. It would place businesses like Apple - whose relationship with customers is in part built on a sense of trust about how data will be handled - in a very difficult position. For the consumer in, say, Germany, this might represent hacking of their data by an Irish business on behalf of the UK state under a bulk warrant - activity which the provider is not even allowed to confirm or deny. Maintaining trust in such circumstances will be extremely difficult.

34. For these reasons, we believe there is a need for much greater clarity as to how the powers in the bill will be applied, not least because, once again, the extension of the powers to overseas providers will set a precedent which, if followed by other countries, could endanger the privacy and security of users in the UK and elsewhere.

Specific Comments on Clauses

Clauses 189, 190 and 191

35. These clauses govern the Secretary of State's ability to require businesses to establish a technical capability to comply with warrants.

36. Paragraphs (1) to (5) of Clause 189 would authorize the Secretary of State to make regulations imposing specified obligations on an operator. Paragraph (4) states that those obligations could include ones "relating to the removal of electronic protection applied by a relevant operator to any communications or data" in other words, the removal of encryption.

37. As set out above, we believe there are significant risks to applying this power to encryption and to extending this power to overseas providers. We therefore do not believe the clause should be retained in its current form and certainly should not extend outside the UK.

38. However, this power could have a very profound effect on any business to whom the clauses apply, and the details are worth examining.

39. First, the oversight seems less rigorous than other parts of the bill. There is no judicial authorization of the requirements placed on businesses. There is no protection for businesses who cannot comply because of local laws.

40. Second, the system does not allow for a full weighing of the costs of compliance. While the clauses require some assessment of compliance cost, it is not clear how this would be calculated. Even if a consensus could be reached on the number of working hours and computing power needed to comply, a proper consideration would need to include the opportunity cost as other projects were put on hold, the knock-on effects for other services and the change in the customer relationship.

41. Third, because (as we explain above) any reduction in encryption in the UK will be exploited by regimes and bad actors not subject to the same privacy and civil liberties protections as UK law enforcement, the implications of a Notice under these clauses would go way beyond either the UK or the affected business. The bill at present does not require any consideration of this.

42. Fourth, there is no explicit obligation for the requirements on a business to be proportionate. Our reading of the bill is that although the Secretary of State might be required to take into account the benefits, costs and technical feasibility of the notice, and consult the Technical Advisory Board and (in the case of review) the Investigatory Powers Commissioner, it is at best implicit that she must only impose requirements that are proportionate. If there is a review, the bill requires that the Investigatory Powers Commissioner must consider whether the notice is proportionate, but the Secretary of State could still reject this advice.

43. The overall effect is a wide ranging power for the Secretary of State to demand a business remove encryption based on an insufficiently robust process and without regard to the full effects, leaving the business with no effective means of appeal.

44. Suggested amendments:

1. The steps required of a business by a Notice should not include removal of electronic protection.
2. These powers should not extend to overseas businesses; a conflict of laws exemption should be added.
3. A notice under s189 should require judicial authorization.
4. There should be clear and concise definitions for the following terms: "removal of electronic protection", "technical feasibility" and "reasonably practicable". These are key terms that should not be left in the first instance for argument in court. Parliament should define and agree what their intent is.
5. The criteria by which the assessment is made by the Secretary of State should be made much more explicit.
6. The Technical Advisory Board advice should be made available to the affected business, and in the case of a review under clause 191, the Interception Commissioner's advice as well.
7. Before imposing any requirement under s189, the Secretary of State should consider whether the time spent in complying, cost (including opportunity cost), knock-on effects and change in customer relationships are reasonable and proportionate to the expected benefits.
8. The Secretary of State should also be obliged to consider the impact of a notice on human rights, in the UK and globally.
9. The Secretary of State should be required only to apply notices that are proportionate as advised by the Commissioner.

<u>Clause 188</u>

45. Paragraph (1) of Clause 188 would authorize the Secretary of State to give any telecommunications operator in the UK a national security notice directing the operator to take such steps as the Secretary of State considers necessary in the interests of national security. 188(4) precludes the powers under this clause being used as a shortcut if powers exist elsewhere in the bill.

46. While we take the strong view that this bill should not be used to demand the removal of encryption, we would not want to see that clarified only for a catch-all Clause 188 to allow the Secretary of State to demand it unilaterally.

47. Suggested amendment:

5. The Clause should be amended to clarify that it cannot be used to require businesses to remove electronic protection from their products or services.

Clause 31

48. This clause places a duty on an operator to comply with a warrant. Again, in line with our argument above, we continue to believe the duty should not be applied to overseas businesses, but have some more general comments on the clause.

49. Clause 31 would require a relevant operator to take all reasonably practicable steps for giving effect to a warrant. Although this is not explicit in the draft bill, our understanding of the government's intention is that this would require us to remove end to end encryption if that was necessary to give effect to the warrant and considered proportionate. The Home Office indicated exactly this in the evidence to your committee we quoted above.

50. In other words, the bill as it stands means that whether or not the Secretary of State has served a business with a Clause189 order requiring it to remove electronic protection, a fresh warrant could be served on a business requiring them to provide data in the clear, backed up by the threat of imprisonment. This seems to represent a short cut for the Secretary of State to insist on removal of encryption - but of course compliance with a warrant in the timescale required by a criminal investigation is likely to be impossible.

51. Suggested amendments:

8. This Clause should not apply to overseas providers.
9. The Clause should be amended to make clear that 'reasonably practicable steps' cannot include removal of electronic protection unless dealt with separately under a Notice under Clause 189, subject to the amendments to that Clause we suggest above.
10. The definition of 'reasonably practicable steps' should be clarified as we set out above to distinguish it from 'technical feasibility.'

Clauses 81 and 135

52. These clauses deal with targeted and bulk equipment interference warrants.

53. We are concerned about the way in which the bill could make private companies implicated in the hacking of their customers.

54. Clause 81(2) provides that a warrant can be served on a person to require them to assist in hacking.

55. Is the intention that persons receiving a warrant would knowingly let the security services break into their equipment or services or allow them to use that equipment to break into equipment used by a third party? Or does the envisaged power go even further and require persons in receipt of a warrant to actively assist in the interference of their own equipment and services?

56. These questions become even more pressing when applied to bulk equipment interference warrants. It is extremely difficult to imagine circumstances in which this could be justified, so we believe the bill must spell out in more detail the types of activities required of communications providers and the circumstances in which they are expected to carry them out. Additionally and in line with earlier comments, these clauses should not have extra-territorial effect.

57. Suggested amendments:

> 11. The powers in this part of the bill need to be fully understood as to their intent. The bill should set out in much more detail what the requirement on a person served with a warrant will be.
>
> 12. The clauses should not apply to overseas providers who would be put in an impossible conflict of laws position.

21 December 2015

ARTICLE 19—written evidence (IPB0052)

Executive summary

1. These are the submissions of ARTICLE 19: Global Campaign for Free Expression ('ARTICLE 19'), an independent human rights organisation that works around the world to protect and promote the right to freedom of expression and the right to freedom of information ('freedom of expression'). ARTICLE 19 monitors threats to freedom of expression in different regions of the world, as well as national and global trends and develops long-term strategies to address them and advocates for the implementation of the highest standards of freedom of expression, nationally and globally.

2. ARTICLE 19 welcomes the opportunity to submit evidence to the Joint Committee on the Draft Investigatory Powers Bill ('draft Bill'). The draft Bill is a once-in-a-generation opportunity to set a blueprint for the world in the protection of privacy and freedom of expression in the context of surveillance. At the outset, however, we note that the Joint Committee has only been offered a limited opportunity to scrutinise the draft Bill as a result of the fast-tracked timetable. We are therefore concerned that insufficient time will be devoted to the draft Bill's implications for the protection of the rights to privacy and freedom of expression. Given the length of the draft Bill and the potential for loopholes, this is a serious concern.

3. In summary, we consider that the draft Bill represents a significant improvement over the Regulation of Investigatory Powers Act 2000 ('RIPA') in terms of transparency and oversight. However, we also consider that it nonetheless fails to deliver the "stringent safeguards" and "world-leading oversight regime" that were promised by the Home Secretary, Theresa May, when the draft Bill was first introduced by the government on 4 November 2015. In particular, we are concerned that:[91]

   (a) the bulk warrantry powers contained in Part 6 of the draft Bill are intrinsically disproportionate in their scope and will have a significant chilling effect on freedom of expression worldwide;

   (b) clause 61 of the draft Bill fails adequately to protect the confidentiality of journalistic sources (including those of non-governmental organisations) and provides no protection whatsoever to a person's confidential communications with doctors and ministers of religion, or the privileged communications of MPs and lawyers;

   (c) the double-lock authorisation procedure provided throughout the draft Bill is too weak to protect the rights to freedom of expression and privacy. Moreover, it does not apply in any event to the acquisition of communications data, the analysis of

[91] In light of the Committee's stated preference to receive short submissions, ARTICLE 19 has confined its evidence to those issues that we regard as being of particular importance. However, the fact that we have not commented on a particular provision cannot be taken as an indication that we agree with it. Rather, this simply reflects the fact that the draft Bill is extremely long whereas we have endeavoured to keep our submissions short.

which may be every bit as intrusive as examining the content of a person's communications; and

(d) the draft Bill contains several provisions of considerable breadth and which lack effective safeguards. In particular, the provisions for equipment interference under Part 5 go beyond mere surveillance and, indeed, are highly intrusive, while clause 189(4)(c) appears to grant the Secretary of State the power to weaken or ban encryption.

The Bulk warrantry powers contained in Part 6 of the draft Bill are intrinsically disproportionate and will have a significant chilling effect on freedom of expression worldwide

4. Part 6 of the draft Bill provides for three different types of bulk warrants: (i) the bulk interception of communications, (ii) the bulk acquisition of communications data; and (iii) the bulk interference with equipment (including personal computers or mobile phone). In each case, the warrants provide for interception, acquisition or interference of an unlimited number of communications, data or devices.

5. There is no requirement whatsoever that the Secretary of State reasonably suspect that those affected are involved in serious crime or threats to national security. Nor is there any requirement that the interference be targeted at a particular person or premises (as is required in the case of warrants issued under clause 13(1)).

6. Nothing in Part 6 or, indeed, elsewhere in the draft Bill imposes any kind of upper limit on what might be obtained by way of a bulk warrant, subject only to the requirement that the Secretary of State considers that it is "necessary" in the interests of national security or certain other specified interests (clauses 107(1)(b)), 122(1)(a), and 137(1)(b)).

7. In other words, it is open to the Secretary of State to issue bulk warrants to obtain potentially billions of emails or phone calls, the data relating to billions of communications, or – indeed – release a computer virus by way of a bulk equipment interference warrant that affects billions of computers or mobile phones without any requirement that s/he believes that those affected may be involved in criminal activity (including terrorism).

8. Although the bulk interception and equipment interference warrants may only be issued where the main purpose of the activity is to acquire intelligence relating to individuals *outside* the UK (clauses 107(3) and 137(3)), this does not prevent potentially millions of persons (and their devices) being affected *within* the UK. Nor is there any corresponding constraint on the ability to obtain bulk communications under Chapter 2 of Part 6 in respect of persons within the UK.

9. The government does not deny that these warrants would involve an interference with the fundamental rights of millions of people who have not been suspected of any

criminal activity of any kind. Instead, its argument is that the material gathered is "likely to include communications or other data relating to terrorists and serious criminals" (para 33 of the Government's Guide to Powers and Safeguards).

10. ARTICLE 19 submits, however, that the fundamental basis of the government's approach is profoundly flawed. The rights to freedom of expression and privacy are simply too important to justify the government collecting the private communications of millions of people it does not suspect of involvement in criminal or terrorist activity. As the Grand Chamber of the European Court of Human Rights held in its recent judgment in *Zakharov v Russia* (47143/06, 4 December 2015), any authorisation for the use of surveillance powers:

> [M]ust be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security (para 260).

11. The fact that bulk interception and acquisition of private communications and the data relating to those communications may be forensically useful is beside the point. In *S and Marper v United Kingdom* [2009] EHRR 50, for instance, the UK government had argued that the retention of DNA samples belonging to people who had not been convicted of any criminal offence was of "inestimable value in the fight against crime and terrorism and the detection of the guilty" (para 91). The Grand Chamber of the European Court of Human Rights in *Marper* did not dispute the UK government's arguments that the DNA material was of "inestimable value". On the contrary, it explicitly recognised "the importance of such information in the detection of crime" (para 106). But the Grand Chamber in that case held that the "blanket and indiscriminate nature of the power of retention" was a disproportionate interference with the right to privacy under Article 8 European Convention on Human Rights ('ECHR') of those persons who had not been convicted of any criminal offence. "Blanket and indiscriminate" retention, the Grand Chamber held, could not therefore be said to be "necessary in a democratic society" (para 125).

12. Similarly in Case C-293/12 *Digital Rights Ireland*, the Grand Chamber of the Court of Justice of the European Union ('CJEU') held that the blanket retention of communications data was a disproportionate interference with the rights to privacy and data protection under Articles 7 and 8 of the EU Charter of Fundamental Rights, involving as it did an "interference with the fundamental rights of practically the entire European population" (para 14).

13. For these reasons, ARTICLE 19 maintains that the bulk warrantry powers set out in Part 6 of the draft Bill are *intrinsically* disproportionate. There is no requirement on the Secretary of State to target the interception or acquisition or interference to those individuals she believes may be involved in serious crime or terrorism. There is no upper limit on the number of people whose private communications may be intercepted or their data gathered. Although Part 6 purports to set restrictions on the circumstances in

which intercepted communications or data may be *examined,* there is no recognition that the very act of intercepting a person's private communications is an interference with their privacy, even if it is not read – just as the Grand Chamber in *Marper* found that there was an interference with a person's privacy merely by having their DNA stored in a database, even if it is never accessed or analysed.

14. As a result, ARTICLE 19 believes that the proposed bulk warrantry powers contained in Part 6 will have a profound chilling effect on freedom of expression. Since the Snowden revelations, for instance, organisations such as ourselves have been obliged to upgrade the security of our communications in order to ensure the confidentiality that our partners, i.e. human rights defenders, journalists and activists, need in order to carry out their work. These concerns are not just theoretical. In *Liberty and others v GCHQ* [2015] UKIPTTrib 13_77-H2, for instance, the Investigatory Powers Tribunal found that GCHQ had intercepted and unlawfully retained the private communications of Amnesty International and the Legal Resources Centre, a South African NGO. Despite the assurances of the Interception of Communications Commissioner that "the interception agencies do not engage in indiscriminate random mass intrusion" (para 6.6.2 of the 2013 report), it has now become clear that NGOs communications worldwide are liable to be intercepted by the intelligence agencies. We cannot understate the risks that this poses to human rights organisations around the world, who rely on the willingness of ordinary men and women to pass them information in confidence, sometimes at their risk to their very lives. The knowledge that the UK intelligences services may intercept those emails – not to mention pass on their contents to a foreign government - is bound to diminish that willingness of people in other countries will have to communicate with NGOs.

15. In July 2014, for instance, Human Rights Watch and Pen International published a report in which it detailed the impact of surveillance on lawyers and journalists in the US.[92] They were told by journalists that government officials were substantially less willing to be in contact with the press.[93] Similarly, lawyers were concerned about their ability to defend their clients in cases in which the intelligence agencies might have an interest.[94] By maintaining a bulk interception and acquisition capability without any requirement of targeting and without adequate safeguards, the UK government is contributing to a global chilling of free expression, including among those NGOs who are working worldwide under dangerous conditions to protect and promote fundamental rights.

16. More generally, the knowledge that our communications might be intercepted, read, analysed by government officials makes individuals more cautious about what they say and how they behave online. It breeds conformity and discourages the most vulnerable to come forward or expression controversial viewpoints. To enshrine mass surveillance programmes into law is likely to result in the public's diminished ability to obtain

[92] See Human Rights Watch and Pen International, *With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law and American Democracy,* July 2014:
https://www.hrw.org/sites/default/files/reports/usnsa0714_ForUPload_0.pdf
[93] *Ibid*. page 3.
[94] *Ibid*. page 4.

information and erosion of our fundamental values as a democratic society. For all these reasons, we believe that the bulk warrantry provisions contained in the draft Bill are simply incompatible with the fundamental values of a democratic society.

The draft Bill fails to provide sufficient protection for confidential information, including journalistic sources and privileged material

17. The importance of protection of journalistic sources as a one of the basic conditions for media freedom cannot be overstated.[95] Media routinely depend on contacts for the supply of information on issues of public interest. Individuals sometimes come forward with secret or sensitive information, relying upon the reporter to convey it to a wide audience in order to stimulate public debate. In many instances, anonymity is the precondition upon which the information is conveyed from the source to the journalist; this may be motivated by fear of repercussions which might adversely affect their physical safety or job security. Journalists would never be able to gain access to places and situations where they can report on matters of general concern if they cannot give a strong and genuine undertaking of confidentiality. If they cannot promise sources anonymity, then they often cannot report at all. When sources are unsure whether they will be protected, they keep silent and the public loses its right to know critical information.[96]

18. Lord Denning recognised the consequences of weak source protection early on. He said "[*I*]*f [newspapers] were compelled to disclose their sources, they would soon be bereft of information which they ought to have. Their sources would dry up. Wrongdoing would not be disclosed. Charlatans could not be exposed. Unfairness would go unremedied. Misdeeds in the corridors of power, in companies or in government departments would never be known*."[97]

19. Up until recent revelations that police had used RIPA to obtain the phone records of reporters to identify sources,[98] journalists could reasonably expect to benefit from strong protections under the Police and Criminal Evidence Act 1984 ('PACE').[99] In general, under PACE, access to journalistic material or confidential sources requires judicial authorisation under Schedule 1 of that Act. We note, however, the report of the inquiry of the Interception of Communications Commissioner in February 2015, in which he found that police forces had used their power to obtain communications data under Part 1 of RIPA in an effort to identify the sources of confidential information received by journalists. Noting that the existing legal framework and practice lacked sufficient procedural safeguards, the Commissioner recommended that access to

[95] See, among leading authorities, *Goodwin v. the United Kingdom*, judgment of 27 March 1996, § 39. For further references, see the European Court of Human Rights factsheet on the protection of journalistic sources: http://echr.coe.int/Documents/FS_Journalistic_sources_ENG.pdf

[96] For more details about the protection of journalistic sources and whistleblowers, see ARTICLE 19's response to the UN Special Rapporteur on Freedom of Expression consultation on protection of journalists' sources and whistleblowers, July 2015: https://www.article19.org/data/files/medialibrary/38082/A19--Protection-of-Sources-and-WBs-Consultation-final.pdf

[97] *British Steel Corpn v Granada Television Ltd*, [1981] 1 All ER 417.

[98] See next para.

[99] See particularly Part 2 (search warrants) and Schedule 1 (special procedure) http://www.legislation.gov.uk/ukpga/1984/60/part/II/crossheading/search-warrants

communications data for the purpose of identifying journalistic sources should be authorised by a judge.

20. In ARTICLE 19's view, however, the requirement for judicial authorisation in clause 61 of the draft Bill in relation to the acquisition of communications data "for the purpose of identifying or confirming a source of journalistic information" (clause 61(1)(a)) fails to provide sufficient protection for the confidentiality of journalistic sources (including those of non-governmental organisations). More generally, we consider that the draft Bill fails to provide adequate protection for other well-established grounds for confidentiality, i.e. doctor-patient, ministers of religion, communications with MPs and legal professional privilege.

21. First, the judicial commissioner is not required under clause 61 to satisfy himself or herself that the access which is sought to the communications data is either necessary or proportionate, having due regard to the need to protect the confidentiality of journalistic sources. Instead, clause 61(5)(a) requires no more than that the judicial commissioner considers that there were "reasonable grounds for considering that the requirements of [Part 3] were satisfied in relation to the authorisation". In ARTICLE 19's view, this is an inadequate safeguard and one that is markedly weaker than that provided under Schedule 1 of PACE in respect of journalistic material. Accordingly, clause 61 creates a perverse incentive for public authorities to rely on the powers under Part 3 of the draft Bill to identify journalistic sources, rather than those under PACE, because the relevant threshold under Part 3 is lower.

22. Secondly, there is no requirement under Part 3 of the draft Bill for an *inter partes* hearing on notice to the journalist concerned. By contrast, any application under Schedule 1 of PACE must be made on an *inter partes* basis (see paragraph 7). There is no obvious reason why – if police wish to seek to identify a journalist's source by means of communications data rather than by way of PACE – the application to obtain the relevant data should be made without giving the journalist an opportunity to be heard. Again, it creates a perverse incentive for public authorities to rely on the powers under Part 3 instead of PACE, since they know that their case will not be vulnerable to any effective challenge.

23. Thirdly, these problems are compounded by the fact that the draft Bill only seeks to protect the 'source of journalistic material', which is narrowly defined. Under clause 61 (7), 'source of journalistic information' means "*an individual who provides material intending the recipient to use it for the purposes of journalism or knowing that it is likely to be so used*". In other words, clause 61 merely seeks to protect the source, i.e. a person, from being identified. By contrast, no provision is made in the Bill for the protection of the 'journalistic material' itself. Indeed, the draft Bill does not attempt to define what 'the purposes of journalism' might involve. It is therefore unclear whether a blogger, civil society organisation or activist could benefit from the limited protections of clause 61. In particular, there is no recognition of the fact that the protection for journalistic sources under Article 10 ECHR extends to NGOs as well as journalists.[100]

[100] See e.g. the European Court of Human Rights, *Gusova v Bulgaria* App. 6987/07, 17 February 2015), at paragraph 38.

While the Information Commissioner's Office has provided guidance as to what may amount to journalistic activity,[101] it is clearly unsatisfactory that the draft Bill fails adequately to make clear the scope of the protection afforded.

24. Fourthly, although provision is made for the protection of journalistic sources, there is no corresponding protection given under clause 61 in respect of communications data that might identify, for instance, details of a person seeking medical advice, religious counselling, or obtaining legal advice. It is simply false to assume that communications data cannot reveal details of such confidential or privileged material. On the contrary, details of a telephone number or website may readily reveal sensitive personal information of this kind, e.g. an AIDS hotline, a website for abortion services, or the time and date that a person contacted a solicitor. The very fact that a person has sought legal advice, for instance, is itself privileged information and yet clause 61 offers no safeguards in this respect.

25. More generally, the draft Bill contains no explicit protection for these categories of confidential information, save that afforded to Members of Parliament under clauses 16 and 85 in respect of warrants for interception and equipment interference. Instead, the government proposes to deal with these categories by way of its Codes of Practice but no draft Codes have yet been published. As it stands, therefore, the draft Bill provides no additional protection for confidential information contained in communications with doctors, ministers of religion, or lawyers.

The double-lock authorisation provides insufficient protection for fundamental rights

26. It is well-established that surveillance powers must be independently authorised, ideally by a judge: see for example the judgment of the European Court of Human Rights (ECtHR) in *Klass v Germany* (1980) 2 EHRR 214:

> The rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and a proper procedure (paragraph 55).

27. Similarly, in *Digital Rights Ireland,* the CJEU stressed the importance of:

> [P]rior review by a court or an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions

[101] https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf

28. In both *Klass* and *Digital Rights Ireland*, it is clear that the decision should be made by a judge and not by a member of the executive who lacks independence from the agencies seeking to carry out interceptions or equipment interference. By contrast, the so-called "double-lock" procedure featured throughout the draft Bill (see clauses 19, 90, 109, 123, 138 and 155) does not confer decision-making power on the judge. Instead, the judicial commissioner is charged only with reviewing the Secretary of State's conclusions as to necessity and proportionality, applying "the same principles as would be applied by a court on an application for judicial review".

29. In ARTICLE 19's view, however, conventional judicial review principles are not adequate to protect fundamental rights in this manner. First, the usual standard applied is *Wednesbury* unreasonableness, which means that the judge cannot disturb the Secretary of State's conclusions as to necessity and proportionality unless he or she is satisfied that the decision was so unreasonable that no reasonable person could have arrived at such a decision. This is an extraordinarily low threshold for the Secretary of State to have to meet, meaning that it is highly unlikely that a judge would ever reverse the Secretary of State's decision.

30. Secondly, the limitations of judicial review are well-established: a judge "may not make fresh findings of fact and must accept apparently tenable conclusions on credibility made on behalf of the authorities."[102] Indeed, a court applying judicial review principles has "no jurisdiction to reach its own conclusion on the primary facts; still less any power to weigh the evidence" (*R(Bewry) v Norwich City Council* [2001] EWHC Admin 657. Indeed, it is for this reason that the European Court of Human Rights has repeatedly found the mere availability of judicial review to be an insufficient safeguard: see e.g. *Tsfayo v United Kingdom* (60860/00, 14 November 2006), in which the Strasbourg Court held that the applicant had not had the benefit of a fair hearing before an independent and impartial tribunal contrary to Article 6 ECHR, notwithstanding that she had had the benefit of judicial review by the High Court, because the High Court "did not have jurisdiction to rehear the evidence or substitute its own views as to the applicant's credibility" (para 48).

31. Thirdly, judicial review principles are an inadequate standard because there is no possibility of an *inter partes* hearing. We are aware of the views expressed by Lord Pannick QC in a recent article in which he expressed the view that judicial review principles provided an adequate basis for the judicial commissioner's review because it was a "flexible" remedy. What Lord Pannick's article ignores, however, is that the more intense, non-standard forms of judicial review have only emerged as a result of *inter partes* argument as to the appropriate threshold or intensity of review to be applied in the particular case. In immigration proceedings, for instance, it will be possible for an applicant to argue that the court should apply a higher threshold than the usual *Wednesbury* standard because of the particular subject matter of the case. In the case of warrants under the draft Bill, by contrast, there is absolutely no prospect of an *inter partes* hearing because to do so would undermine the secret nature of surveillance. There is, therefore, no realistic prospect that a judicial commissioner would conclude

[102] *Runa Begum v London Borough of Tower Hamlets* [2003] UKHL 5.

that a higher level of review than *Wednesbury*-unreasonableness should apply, especially as the judicial commissioner would have no opportunity to hear oral argument on the issue. More to the point, there is absolutely nothing in the draft Bill that would permit a judicial commissioner to apply a higher standard. In other words, the so-called double lock is in reality a single lock, and it is the Secretary of State who has the key.

32. We note, in any event, that even the weakened judicial approval mechanism contained in the draft Bill does not apply to the acquisition of communications data, save as provided by clause 61 or where it is sought by way of a bulk warrant under Chapter 2 of Part 6. Given the obvious sensitivity of communications data and its ability to disclose highly sensitive details of a person's private life, [103] we regard this as entirely unsatisfactory.

33. Lastly, ARTICLE 19 notes that many other countries around the world, such as Canada and the United States, have judicial authorisation of interception, in which the judge takes the relevant decision alone, and yet there is no evidence of any lack of effectiveness of surveillance in those jurisdictions. More generally, we are concerned that – by establishing an unduly weak model of judicial oversight – the United Kingdom is liable to set a poor example to other countries who are likely to be influenced by the model adopted here. If the Home Secretary's claim to deliver "world-leading" oversight is to have any substance, the draft Bill must contain actual judicial authorisation rather than just mere judicial review.

The draft Bill grants powers of undefined scope without sufficient safeguards

34. In addition to our concerns outlined above, ARTICLE 19 notes that the draft Bill contains a number of provisions of considerable breadth and which lack effective safeguards. These include the use of warrants for equipment interference under Part 5 and Chapter 3 of Part 6, the provision for national security notices under clause 188 and for the maintenance of technical capabilities under clause 189.

35. Firstly, ARTICLE 19 notes that the new equipment interference powers under parts 5 and 6 of the draft Bill present significant challenges for investigative journalism. Equipment interference (i.e. hacking), whether carried out by a government or private actor, is perhaps the most serious form of intrusion into someone's private life, given that it involves access to private information without permission or notification. It also fundamentally breaches the integrity of the target's own security measures. Unlike search warrants where the individual would at least be notified that their home or office was being searched, hacking generally takes place without a person's knowledge. It is the equivalent of the police breaking into someone's home. The 'interference' with equipment takes on different forms, from logging keystrokes on a computer to identify a password to taking control of someone's smartphone covertly to take photographs or record video or sound without the user or owner's knowledge.

[103] See NSA General Counsel Stewart Baker *"metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content."* as quoted in Techdirt, *Michael Hayden Gleefully Admits: We Kill People Based on Metadata,* 12 May 2014, available at: https://www.techdirt.com/articles/20140511/06390427191/michael-hayden-gleefully-admits-we-kill-people-based-metadata.shtml

36. Given the obvious intrusiveness of such a measure, it should only be authorised by a judge in the most exceptional circumstances and must be subject to strict conditions. In particular, hacking should only be available for the most serious offences and as a last resort, once other, less intrusive methods have already been exhausted. However, under the draft Bill, these powers are merely subject to the 'double lock' provision mechanism whose weaknesses have already been referred to.

37. Secondly, clauses 188 and 190-191 make fresh provision for the Secretary of State to issue national security notices in secret to telecommunications providers, replacing the existing power under section 94 of the Telecommunications Act 1984. We note that the power under section 94 was so broad that it was used by intelligence services to obtain stored communications in bulk. The Explanatory Notes state that bulk acquisition warrants in Part 6 "replaces the provision at section 94 of the Telecommunications Act 1984 which will be repealed". What the Explanatory Notes do not say, however, is that – although the power in the 1984 Act will be repealed – it is effectively replicated by clauses 188 and 190-191. In ARTICLE 19's view, the very fact that the vaguely-worded power contained in section 94 could be used by the intelligence services to secretly obtain sensitive personal data on an industrial scale is the best argument against its reinstatement in the draft Bill. Despite this, we note that the draft Bill contains very little in the way of safeguards to prevent similar abuse in future.

38. Thirdly, we have similar concerns about the proposed power of the Secretary of State under clause 189 to make regulations imposing "specified obligations on relevant operators", including "*obligations relating to the removal of electronic protections applied by a relevant operator to any communications or data*" under clause 189(4)(c). Despite the Government's assurances that the draft Bill would not include 'backdoors' and that encryption would continue to be protected, it is apparent that the *vires* of clause 189(4)(c) are sufficiently broad to enable the Secretary of State to make regulations requiring operators either to remove encryption services upon request, or to reduce the effectiveness of encryption. This would fundamentally undermine the use of end-to-end encryption and therefore the security of our online communications and transactions. In practice, it is equivalent to a government 'backdoor'.

39. In ARTICLE 19's view, the continuing availability of strong, end-to-end encryption is essential to the protection of privacy and free expression in the digital era. As the UN Special Rapporteur on Freedom of Expression recommended in his May 2015 report:

> 59. States should promote strong encryption and anonymity. National laws should recognize that individuals are free to protect the privacy of their digital communications by using encryption technology and tools that allow anonymity online. Legislation and regulations protecting human rights defenders and journalists should also include provisions enabling access and providing support to use the technologies to secure their communications.
>
> 60. States should not restrict encryption and anonymity, which facilitate and often enable the rights to freedom of opinion and expression. Blanket

prohibitions fail to be necessary and proportionate. States should avoid all measures that weaken the security that individuals may enjoy online, such as backdoors, weak encryption standards and key escrows.

40. The breadth of the powers afforded to the Secretary of State under clauses 188 and 189 are compounded, in our view, by equally vague definitions under chapter 2 of Part 9. Although the Home Secretary has referred to the draft Bill containing "stringent safeguards", there are few apparent restrictions on the power of the Secretary of State under Part 9 to issue directions in secret or make regulations that would weaken or undermine the use of strong end-to-end encryption in the UK.

18 December 2015

Bar Council—supplementary written evidence (IPB0134)

1. This is the response of the General Council of the Bar of England and Wales (the Bar Council) to the questions posed by the Joint Parliamentary Committee on the Draft Investigatory Powers Bill. This paper serves as the Bar Council's submission of written evidence to the Joint Committee.

2. The Bar Council represents over 15,000 barristers in England and Wales. It promotes the Bar's high quality specialist advocacy and advisory services; fair access to justice for all; the highest standards of ethics, equality and diversity across the profession; and the development of business opportunities for barristers at home and abroad.

3. A strong and independent Bar exists to serve the public and is crucial to the administration of justice. As specialist, independent advocates, barristers enable people to uphold their legal rights and duties, often acting on behalf of the most vulnerable members of society. The Bar makes a vital contribution to the efficient operation of criminal and civil courts. It provides a pool of talented men and women from increasingly diverse backgrounds from which a significant proportion of the judiciary is drawn, on whose independence the Rule of Law and our democratic way of life depend. The Bar Council is the Approved Regulator for the Bar of England and Wales. It discharges its regulatory functions through the independent Bar Standards Board

Contents and summary

Introduction

4. The Bar Council considers that the Bill will provide a much-needed opportunity to provide a clear legislative basis for intrusive investigations into the activities of persons in this country. When the state engages in such investigations, it must do so under the cover of law, clearly set out in statute, clearly understood by investigators and the public, and clearly and transparently enforced by the courts. Any failure to achieve these conditions creates a sense that the authorities and the security services in particular are immune from lawful constraint. That cannot be allowed to exist in a democratic state, which depends upon trust and co-operation from its citizens.

5. No government can be allowed to interfere with the privacy of its citizens at will. Only authoritarian states employ arbitrary arrest, restrictions on freedom of expression or of communication. Unless authorised by law, and subject to a transparent process of confirmation of the legitimacy of the action, the powers contained in this Bill would be arbitrary and undemocratic.

6. One of the essential rights in a democracy is the right of a citizen to consult with a lawyer. For that right to have any meaning, especially when it so often occurs in circumstances when the citizen is in some form of legal dispute with the state, the citizen must have private access to effective independent legal advice. The expression "Legal Professional Privilege" is used to describe this right. It is not the right of lawyers – lawyers are its servants not its owners. The privilege is that of the client, and failure to protect that right against the state amounts to a significant inroad into a long-standing principle, which has formed an important foundation of our rule of law.

7. The Bill contains some wide-ranging powers. Some of these powers raise questions about practicality, namely, whether the information gathered can be kept secure from access by malign individuals and organisations. These are essentially practical matters which others are better placed to address. Failure to address them will risk intrusion in to people's privacy to an extent which Parliament would not sanction.

Legal Professional Privilege (LPP)

8. Legally privileged communications are those between a client and their lawyer which come into existence for the dominant purpose of being used for legal advice or in connection with actual or pending litigation.

9. When the law allows the state to eavesdrop on privileged communications to gather intelligence, clients feel unable to speak openly with their lawyers. The result is that defence teams may not know about perfectly proper defences open to a defendant and will therefore not advance them at trial. Breaching privilege also carries the risk that those guilty of offences are not successfully prosecuted because of the risks to the integrity and fairness of criminal and civil trials.

10. Legal privilege does not apply where communications between a lawyer and client are made for the furtherance of criminal activity.

11. The Bar Council recognises that the antiquity of LPP is not by itself a sufficient reason why it should be given protected status. So why is it important? It is a cornerstone of civil society, governed by the rule of law, that persons are able to consult a legal adviser in absolute confidence, knowing there is no risk that information exchanged will become known to third parties without the client's clear authority. The government acknowledged the importance of LPP in *Belhadj* [2015] UKIPTrib 13_132_H @ [13].

> 'There was no dispute between the parties as to the importance of protecting and preserving the concept of legal and professional privilege, as clarified or enunciated particularly in R v Derby Justices ex p B [1996] AC 487 at 507, R (Morgan Grenfell) v Special Commissioners [2003] 1 AC 563 at paragraph 39 and R v Grant [2006] QB 60 at paragraphs 52 and 54.'

12. When privilege is breached, so are our fundamental rights. The Security Services admitted in 2015 to having spied on legally privileged communications. This was permitted under Regulation of Investigatory Powers ("RIPA") and the House of Lords ruling *Re McE* [2009] UKHL 15 but, as the security services later admitted, such surveillance activities were also unlawful. It is not sufficient that, if it becomes known that LPP material has been obtained by the state, such material is inadmissible. As is obvious, the individual whose privileged material is intercepted or accessed will not know about it. Even if it comes to light during litigation, an unfair advantage is likely to have been obtained by the state. Worse, if it is passed on to foreign states, it might be used for purposes of which we disapprove.

13. In the case of *McE* in the House of Lords, Lord Phillips (who dissented from the majority judgment) described the "chilling" effect on the administration of justice if LPP is not protected. Those of us who have appeared in cases involving allegations of terrorism offences have experienced this effect. The administration of justice requires independent judges who in turn rely on independent lawyers who are able to give robust advice to their clients. Such advice will not be possible when clients fear – as they do – that everything they say to their lawyers goes straight to the Security Services or the police.

14. There was nothing in RIPA expressly to sanction access to LPP material. The fact that this Bill employs identical wording (e.g. in section 5 and 65 – "lawful for all purposes") to that in section 27 of RIPA, and which the House of Lords in *Re McE* decided was sufficient to demonstrate Parliament's intention to displace LPP as an exception, means that the Home Office intends that this Bill will have the same effect. If that is their intent, it should be stopped. The best way to achieve that is to include express protection in the Bill as in the statutes referred to below. Why is the Home Office unwilling to put into the body of this Bill protection for LPP which has featured in many other statutes – e.g. The Police and Criminal Evidence Act 1984, The Terrorism Act 2000, the Police Act 1997, the Criminal Justice and Police Act 2001 and the Proceeds of Crime Act 2002? Attached as an Appendix is a draft set of amendments to correct this omission.

15. The Bill contains added protection for MPs and for journalistic material to some extent. There is nothing in the body of the Bill to protect LPP which, in international and domestic law, has always been regarded as deserving greater protection from the state. The Home Office offers the consolation that LPP will be protected in the Codes of Practice. They have the force of law, but not to the same extent as primary legislation.

Response to questions

Question 1: Aside from the new powers on the retention of Internet connection records, does the draft Bill consolidate existing powers or does it extend them?

16. The ability to obtain bulk warrants is an extension. These warrants may be non-specific as to individuals or locations or equipment. The question will be whether applications for such warrants can satisfy the tests of necessity and proportionality. Bulk search warrants or bulk arrest warrants would not. A high level of justification should be required for these bulk warrants to determine why focused warrants with the power to amend and extend in the light of information gathered would not be sufficient in order to satisfy the tests of necessity and proportionality.

Question 2: What test do you think is meant by applying "the same principles as would be applied by a court on an application for judicial review"? Is this sufficiently clear in this context for consistent decision-making? Would you describe the application of this test as a "double-lock"?

17. Lawyers generally agree that the test to be applied when dealing with activity which intrudes upon a person's Convention rights, as these powers do, is one of a re-assessment on the merits. This involves more than a review of whether the Secretary of State has made an illogical decision or one beyond her/his powers. If that is the intention, then the reference to judicial review is superfluous and should be deleted to avoid possible misconstruction. If the words mean something else, then they should be deleted as being an undesirable fetter on the Judicial Commissioner's role.

Question 3: Is five days a proportionate amount of time for the Secretary of State to seek the approval of a Judicial Commissioner under the urgent application procedure?

18. The Bar Council can see no justification for allowing an unauthorised warrant to exist for up to five days. High Court Judges frequently listen to and grant orders made on urgent application. Provided sufficient Commissioners are appointed there is no reason why they would not be at least as available to make a decision as the Secretary of State.

Question 4: How can Judicial Commissioners ensure they retain their cultural independence?

19. The Bar Council is confident that any Commissioner appointed from the High Court or above would retain independence. It is desirable that a number of Judicial Commissioners are appointed in order for them to create a collegiate body of experience.

Question 5: Do the terms of appointment for Judicial Commissioners sufficiently guarantee their independence from the executive?

20. The Bar Council suggests that these judicial appointments should be made by the by the Judicial Appointments Commission, in consultation with the Lord Chief Justice.

Question 6: How do you anticipate the power of the Secretary of State to modify the "functions" of the Judicial Commissioners would be used?

21. These powers (which would include the power to add to the remit of the Commissioners' functions should there be any future statutory provisions requiring their attention) should be confined to sections 169, 173 and 174. There should be no power in the Secretary of State to amend the Commissioners' main functions. That should be for Parliament to consider by primary and not subordinate legislation.

Question 7: What would be the best way to fund the Judicial Commissioners to ensure their independence, both real and perceived, from the Government?

22. The Commissioners should retain their judicial salary or the equivalent in the case of retired judges. The funding for the establishment of the Commissioners' might be a matter for the Home Office to propose and a Parliamentary Committee to approve. No doubt the Investigatory Powers Commissioner will include in an annual report any problems caused by lack of funding.

Question 8: Do the oversight mechanisms in the draft Bill satisfy the requirements of Article 8 of the European Convention on Human Rights?

23. There are two areas in which the Bill might fail an Article 8 test.

23.1 The first is the failure to protect LPP. The jurisprudence in Strasbourg does not go as far as the common law in treating LPP as an absolute right (subject to an express restriction by Parliament). However, the importance of LPP as an adjunct to the right to legal advice is recognised. LPP engages Article 6 as well as Article 8. In the context of the circumstances in which the powers under this Bill will be exercised, there is likely to be a consequential conflict with either or both Article 8 and Article 6 in that the results of the execution of the warrants might be arrest and prosecution or the use of restrictive powers over a person's movements and contacts.

23.2 The second is the potential width of bulk warrants, and whether they will satisfy the test of legal certainty required under both Articles.

Question 9: Does the draft Bill address concerns about legal professional privilege and investigatory powers? Does it create any new issues in relation to LPP? How would you address any outstanding concerns?

24**.** As set out above, the Bar Council is concerned at the absence of express protection for LPP in the Bill. Bulk interception warrants require careful assessment as they might capture LPP material. Communications data, although confined to data not content, will also capture LPP material. The contact details of the person a lawyer contacts immediately after speaking to his/her client will indicate the identity of a witness and possibly the subject-matter of the conversation. We propose that express provision be made in the Bill along the lines of those provisions in PACE and TACT and the Police Act 1997 as in the Appendix to this Response.

Question 10: What is the legal status of the Codes of Practice under RIPA? What do you expect to be contained in the Codes of Practice issued under this Bill?

25. The Codes do have the force of law, but not the same force as primary legislation. Primary legislation governs what is permissible in codes of practice. The Codes did not prevent the unlawful acts identified in *Belhadj*. The Home Office has said that it intends to place protection of LPP in a Code, as it has in the current draft RIPA code. However, that protection does not adequately protect LPP. In fact it does not treat LPP as immune from authorised examination. Previous legislation (as above) requires the state to avoid accessing LPP material, or, if it is unavoidably mixed in with material which is the legitimate subject of investigation, then provision is made to isolate it and make it subject to independent legal examination to confirm whether or not it is protected by LPP. If it is, then it is not accessible by investigators and must be destroyed or deleted.

26. Primary legislation should make clear the distinction between deliberate access to LPP material (including obtaining access when it is known to be likely that the communication is subject to LPP) and inadvertently accessing it as part of an otherwise legitimate execution of a warrant. Schedule 6 contains the sole reference in the Bill to material subject to LPP. Paragraph 4(1)(b) provides –

> (1) A code of practice about the obtaining or holding of communications data by virtue of Part 3 must include—
>
> (b) provision about particular considerations applicable to any data which relates to a member of a profession which routinely holds legally privileged information …

27. This indicates (as is known from proceedings before the Investigatory Powers Tribunal) that the Security and Intelligence Services are able to identify who is likely to be in possession of LPP.

28. Why is this restriction on access in the Codes restricted to communications data? Why is there not to be a similar provision for intercepts? The words *particular considerations* do not demonstrate a desire in the Home Office to respect the government's agreement in *Belhadj* [paragraph 12 above] about the importance of LPP.

Question 11: What practical effect is the introduction of a right of appeal from the Investigatory Powers Tribunal likely to have?

29. The Bar Council supports the right of appeal. It will enable the development of a body of jurisprudence concerning the exercise of these exceptional procedures to build on the reasoned decisions of the Tribunal. A right of appeal may also enable the IPT do deal more summarily with cases it regards as frivolous.

Question 12: Why is it important that the Investigatory Powers Tribunal is able to hold as much of its proceedings in public as possible?

30. Justice which is partly secret justice is occasionally necessary to protect the safety of others, and sometimes for reasons of national security. When it is not essential, open justice which can be subject to rational (and sometimes irrational) scrutiny is an essential part of

ensuring that the public have confidence in the process of what is otherwise a closed system.

Question 13: Is it appropriate that material acquired from targeted equipment interference warrants may be used as evidence in legal proceedings? Is it desirable?

31. The Bar Council understands the arguments deployed by the Home Office about the difficulties of routine use of such material in evidence. However, the Bill allows such material to be used in the tribunals set out in Schedule 3 (see section 42(1)), namely the IPT, SIAC, etc. If the intercept material can be used in those tribunals, presumably predominantly to support the government's case, it is difficult to see why it cannot be used in non-closed proceedings, even if the process by which it has been obtained is not in evidence nor disclosed to the accused. There have now been numerous reports on this matter, and the use of it in closed proceedings only is unsatisfactory. The absolute prohibition on use of this material in certain cases of serious crime risks failure to do justice to victims and potential victims of e.g. modern slavery offences.

Question 14: Is the retention of data for 12 months a proportionate balance between the needs of the security services and law enforcement and the rights of the individual?

32. Subject to there being adequate safeguards about unauthorised access to that retained material, 12 months seems a proportionate period. In the absence of evidence about what will and what will not be achieved by such a period as distinct from any other period, it is difficult to express a concluded view.

Question 15: Does clause 13(2) meet common law and ECHR requirements as to the detail to be included in warrants and is it sufficiently clear in its terms, for example in explaining what is meant by group etc. or does it require significant amendment if it is to remain in the Bill?

33. Provided that the group, organisation or premises are identified with sufficient precision, clause 13(2) should satisfy the ECHR requirements of certainty. A warrant expressed in general terms e.g. "anyone suspected of involvement in money laundering in London" would not be compliant.

34. It is at this stage that the role of the Judicial Commissioner becomes critical. (S)he must ensure that the warrant is confined in time, location, persons and subject-matter to avoid the warrant becoming what might be described as a "willy-nilly" warrant. Unless precision is contained within the warrant, it should not satisfy the dual tests of necessity and proportionality which the Judicial Commissioner is to apply by clause 19(1). Unless the warrant is sufficiently precise, it will be impossible to monitor whether it has been lawfully executed. In the light of the immunity created by clauses 5 and 65 for acts covered by a warrant ("lawful for all ... purposes"), it is essential that the persons executing the warrant, the Judicial Commissioner, and, in hindsight a court or tribunal, is able to ascertain the precise limits of authority set out in the warrant. Unless its legality can be tested by monitoring, the use of this power will fail the test of necessity and proportionality. That

conclusion should guide the Judicial Commissioners in the exercise of their function under clause 19.

Question 16: Should the present powers relating to bulk interception warrants be replicated in the draft Bill or should warrants be more narrowly focused as to their purpose and permitted search criteria?

35. Part 6 of the Bill will regulate the power to issue bulk interception warrants. By clause 106 such warrants are confined to communication from or to an individual who is outside the British Islands. This necessarily implies that the other or others involved in the communication are located within the British Isles and therefore entitled to the protection of English (or Scottish or Northern Irish) law, including the Convention rights in the Human Rights Act.

36. Clause 107 authorises the Secretary of State to issue such a warrant if satisfied that the "main" purpose of the interception is to intercept "overseas-related communications" and to obtain related communications data from such communications. This is a very wide power, especially given the protean definition of "data" in clause 195(1). The ambit of the warrant is however narrowed by clause 107(2)-(5). These sub-clauses include a condition that the warrant must be directed to obtain information about the acts or intentions of a person outside the British Islands.

37. In what appears to be a type of "snakes and ladders" exercise in legislative drafting, clause 107(1)(d), (2) and (6) require that the Secretary of State must consider that examination of the material or data is necessary for a "specified operational purpose" concerned with preventing or detecting serious crime or in the interests of the economic well-being of the United Kingdom. Clause 111 further requires that the operational purposes must be specified, and that it is not sufficient to use the generic mantra "preventing or detecting serious crime or in the interests of the economic well-being of the United Kingdom". But then clause 111(4) says that other general purposes *will* suffice.

38. Similar considerations about the dangers of failing to specify the targets and the subject-matter identified in the answer to Question 15 apply to bulk interception warrants.

Appendix 1: Draft Investigatory Powers Bill initial draft New Clauses Proposed by the Bar Council for the protection of Legal Professional Privilege.

<u>Targeted and bulk interception of Communications: New Clause after Clause 17</u>

`Matters subject to legal privilege

(1) A warrant under this Chapter, or under Chapter 1 of Part 6, may not authorise conduct undertaken for the purpose of doing anything in relation to—

(a) a communication, insofar as the communication consists of matters subject to legal privilege;

(b) related communications data, insofar as the data relate to the communication of matters subject to legal privilege.

(2) In subsection (1), "matters subject to legal privilege" means matters to which section 98(2), (3) or (4) of the Police Act 1997 applies, but does not include a communication made with the intention of furthering a criminal purpose.

(3) For the purposes of subsection (2)—
(a) a communication is not to be treated as made with the intention of furthering a criminal purpose unless there is compelling evidence to that effect;
(b) the Secretary of State may by regulations make provision for the determination by a Judicial Commissioner, on an application for a warrant or otherwise, of the question whether in any case a communication is made with the intention of furthering a criminal purpose.

(4) A code of practice issued under Schedule 6 must contain provision about—
(a) the steps to be taken to minimise the risk of conduct undertaken pursuant to a warrant to which this section applies resulting in accidental acquisition of a communication, or communications data, falling within subsection (1);
(b) the steps to be taken if it appears that such conduct has accidentally resulted in acquisition of such a communication or data.'

Targeted and bulk acquisition of communications data: New Clause after Clause 65

Matters subject to legal privilege

(1) An authorisation under this Part, or under Chapter 2 of Part 6, may not authorise or require anything to be done for the purpose of obtaining or disclosing communications data relating to the communication of matters subject to legal privilege.

(2) In subsection (1), "matters subject to legal privilege" means matters to which section 98(2), (3) or (4) of the Police Act 1997 applies, but does not include a communication made with the intention of furthering a criminal purpose.

(3) For the purposes of subsection (2)—
(a) a communication is not to be treated as made with the intention of furthering a criminal purpose unless there is compelling evidence to that effect;
(b) the Secretary of State may by regulations make provision for the determination by a Judicial Commissioner, on an application for authorisation or otherwise, of the question whether in any case a communication is made with the intention of furthering a criminal purpose.

(4) A code of practice issued under Schedule 6 must contain provision about—
(a) the steps to be taken to minimise the risk of conduct undertaken pursuant to an authorisation to which this section applies resulting in accidental acquisition of communications data, falling within subsection (1);
(b) the steps to be taken if it appears that such conduct has accidentally resulted in acquisition of such data.'

Equipment interference: New Clause after Clause 103

`Matters subject to legal privilege

(1) A warrant under this Part, or under Chapter 3 of Part 6, may not authorise or require anything to be done for the purpose of intercepting, obtaining communications data about, selecting for examination, or disclosing, any communication of matters subject to legal privilege.

(2) In subsection (1), "matters subject to legal privilege" means matters to which section 98(2), (3) or (4) of the Police Act 1997 applies, but does not include a communication made with the intention of furthering a criminal purpose.

(3) For the purposes of subsection (2)—
(a) a communication is not to be treated as made with the intention of furthering a criminal purpose unless there is compelling evidence to that effect;
(b) the Secretary of State may by regulations make provision for the determination by a Judicial Commissioner, on an application for authorisation or otherwise, of the question whether in any case a communication is made with the intention of furthering a criminal purpose.

(4) A code of practice issued under Schedule 6 must contain provision about—
(a) the steps to be taken to minimise the risk of conduct undertaken pursuant to a warrant to which this section applies resulting in the accidental intercepting, obtaining communications data about, selecting for examination, or disclosing, any communication falling within subsection
(b) the steps to be taken if it appears that such conduct has accidentally resulted in any of those things.'

Surveillance and covert human intelligence sources: New Clause after Clause 192

`Surveillance and covert human intelligence sources: legal privilege

Amendment of Regulation of Investigatory Powers Act 2000

In section 27 of the Regulation of Investigatory Powers Act 2000 (authorised surveillance and human intelligence sources), after subsection (4) insert—

(5) An authorisation under section 28 or 32 may not authorise surveillance for the purpose of obtaining information about—

(a) anything taking place on so much of any premises as is in use for the purpose of legal consultations, or

(b) matters subject to legal privilege.

(6) An authorisation under section 29 does not authorise any activities involving conduct of a covert human intelligence source, or the use of such a source, for the purpose of—

(a) obtaining matters subject to legal privilege,

(b) providing access to any matters subject to legal privilege to another person, or

(c) disclosing matters subject to legal privilege.

(7) In subsection (5), "legal consultation" means -

(a) a consultation between a professional legal adviser and his client or any person representing his client, or

(b) a consultation between a professional legal adviser or his client or any such representative and any other person made in connection with or in contemplation of legal proceedings and for the purpose of such proceedings, except in so far as the consultation consists of anything done with the intention of furthering a criminal purpose.

(8) In subsections (5) and (6), "matters subject to legal privilege" means matters to which section 98(2), (3) or (4) of the Police Act 1997 applies, but does not include anything done with the intention of furthering a criminal purpose.

(9) For the purposes of subsection (8)—

(a) a communication is not to be treated as made with the intention of furthering a criminal purpose unless there is compelling evidence to that effect;

(b) the Secretary of State may by regulations make provision for the determination by a Judicial Commissioner (within the meaning of the Investigatory Powers Act 2016), on an application for authorisation or otherwise, of the question whether anything referred to in subsection (7) or (8) is done with the intention of furthering a criminal purpose.

(10.) A code of practice issued under section 71 may in particular contain provision about—

(a) the steps to be taken to minimise the risk of conduct undertaken in reliance on this Part accidentally resulting in information of a kind mentioned in subsection (5) being obtained or in any of the things mentioned in subsection (6)(a), (b) or (c) being done;

(b) the steps to be taken if it appears that such conduct has accidentally resulted in such information being obtained or such things being done."'

Explanatory note on the wording of the New Clauses

1. These new provisions would operate by preventing the *targeting* of legally privileged material. It would be impermissible for a warrant or authorisation to enable any actions for the *purpose* of obtaining privileged information.

2. The obtaining of privileged information cannot be removed entirely from the scope of authorisation because, as pointed out by the Lords in *Re McE*, it may only become apparent to the authorities that privileged information has been obtained once they have received the fruits of the operation. Instead, the new Clauses deploy the Codes of Practice issued under the draft Bill, and under RIPA section 71, as a source of guidance on minimising the risk of accidently obtaining legally privileged material and dealing with the consequences of having obtained it.

3. The provisions all define "matters subject to legal privilege" by cross-referring to Police Act 1997 section 98(2), (3) and (4). That was the approach taken by the Government in the Covert Human Intelligence Sources: Matters Subject to Legal Privilege Order 2010.

4. The 1997 Act's exceptions from LPP have been adjusted for the purpose of these New Clauses. Section 98(5) of that Act takes matters out of LPP if the item or communication in question is (a) "in the possession of a person who is not entitled to them" or (b) "held, or… made, with the intention of furthering a criminal purpose." That would be counter -productive in relation to privileged material accessed by a CHIS, because a person such as an undercover police officer is plainly *not* entitled to the privileged information, yet it is precisely in this situation that LPP needs to be preserved. So the Clauses focus on of criminal intention.

5. Included in the Clauses is provision enabling the Secretary of State to make regulations to determine the application of the iniquity exception. That question would most likely arise on an application for authorisation, where the authorities have grounds to suspect that privilege is being abused. But it might also arise later in an investigation when the fruits of the covert operation are found to include lawyer-client communications which it appears might attract the iniquity exception. Hence the "or otherwise" wording. Those subsections expressly confine the regulations to providing for determinations for the purposes of the relevant sections of the Bill or RIPA. So a decision about the iniquity exception under these provisions could not bind the person deciding any equivalent issue arising in, for example, a criminal trial.

Bar Council[104]

Appendix 2: Supplementary written evidence to the Joint Parliamentary Committee on the Draft Investigatory Powers Bill

Further supplementary written evidence

[104] Prepared by the Surveillance and Privacy Working Group on behalf of the Bar Council

1. This is the response of the General Council of the Bar of England and Wales (the Bar Council) to the additional questions posed by the Joint Parliamentary Committee on the Draft Investigatory Powers Bill as set out in the document sent by email on 17th December 2015 to Peter Carter QC by Hannah Stewart, Legal Specialist, Scrutiny Unit, House of Commons. This paper serves as the Bar Council's supplementary submission of written evidence to the Joint Committee.

2. **Question 1:** Do the oversight mechanisms in the draft Bill satisfy the requirements of Article 8 of the European Convention on Human Rights?

3. This is the same as the original question 8 and is contained within the Bar Council's previous submission.

4. **Question 2:** What is the legal status of the Codes of Practice under RIPA? What do you expect to be contained in the Codes of Practice issued under this Bill?

5. This is the same as the original question 10 and is contained within the Bar Council's previous submission.

6. **Question 3:** What practical effect is the introduction of a right of appeal from the Investigatory Powers Tribunal likely to have?

7. This is the same as the original question 11 and is contained within the Bar Council's previous submission.

8. **Question 4:** Why is it important that the Investigatory Powers Tribunal is able to hold as much of its proceedings in public as possible?

9. This is the same as the original question 12 and is contained within the Bar Council's previous submission.

10. **Question 5:** Is it appropriate that material acquired from targeted equipment interference warrants may be used as evidence in legal proceedings? Is it desirable?

11. **Question 6:** Is there an on-going justification for intercept material remaining inadmissible in legal proceedings?

12. Questions 5 and 6 raise similar issues to those in the original Q 13 and which are contained within the Bar Council's previous submission.

13. **Question 7:** The Bill creates a new offence of disclosing the fact that warrants for equipment interference have been authorised and that such activities have taken place (Clause 102). Will this have any impact on legal proceedings in your view?

14. This raises similar issues to those considered in response to questions 5 and 6. It also raises issues which are the subject of Additional questions 11 and 12 which are answered below.

15. **Question 8:** Is the retention of data for 12 months a proportionate balance between the needs of the security services and law enforcement and the rights of the individual?

16. This is the same as the original question 14 and is contained within the Bar Council's previous submission.

17. **Question 9:** Does clause 13(2) meet common law and ECHR requirements as to the detail to be included in warrants and is it sufficiently clear in its terms, for example in explaining what is meant by group etc. or does it require significant amendment if it is to remain in the Bill?

18. This is the same as the original question 15 and is contained within the Bar Council's previous submission.

19. **Question 10:** Should the present powers relating to bulk interception warrants be replicated in the draft Bill or should warrants be more narrowly focused as to their purpose and permitted search criteria?

20. This is the same as the original question 16 and is contained within the Bar Council's previous submission.

21. **Question 7:** The Bill creates a new offence of disclosing the fact that warrants for equipment interference have been authorised and that such activities have taken place (Clause 102). Will this have any impact on legal proceedings in your view?

22. **Question 12:** Section 102 creates an offence of unauthorised disclosure of equipment interference warrants. What impact could this have to the disclosure obligations under the Criminal Procedure and Investigations Act 1996? What is your opinion of the hypothesis that defendants will routinely allege hostile equipment interference on their computers and smart phones by law enforcement and that defence lawyers will then seek to have such evidence excluded for unreliability and potential contamination under s 78 PACE?

23. Clause 102 creates an offence of disclosing anything about equipment interference warrants. The offence is confined to disclosure by the relevant telecommunications provider. This must be seen in conjunction with clause 42 which prohibits any evidence to be adduced or question asked by anyone in legal proceedings (except those in closed sessions in SIAC, the IPT etc) about warrants for lawful interceptions or the associated data. Clause 42 is the subject of our previous submission on original Q 13. There is however an additional factor involved in equipment interference, namely the possibility that the process of interference might affect the integrity of the equipment and of the data obtained from it. Technical experts will need to explain how warranted interference – targeted or bulk – can avoid affecting the integrity of any particular device which is subsequently seized, imaged for investigation purposes and then placed in evidence. If it becomes critical to a criminal prosecution to proved that D deliberately accessed a particular site, can the fact that a

warranted interference was taking place simultaneously exclude the possibility that the interference itself contributed to the download of material from that site?

24. If this is not a realistic possibility, the fact remains that some defendants might allege it. If that occurs the point will inevitably engage the courts in disputes about disclosure and may require detailed expert evidence. The government's customary stance of "neither admit nor deny" will encourage the belief in some defendants that interference was not confined to acquiring information communications and data as identified in clause 81, namely

a. communications (see section 105),
b. private information (see section 105), and
c. equipment data (see section 82).

but also extended to remote control of the equipment.

25. Many of the items of equipments which are subject to interference warrants will be in multiple use. Disentangling who is responsible for which communication is often a problem. This will again give rise to disclosure issues; contiguous communications can identify a particular user, who may not be the defendant. The material obtained by warrant might include such exculpatory details.

26. **Question 11:** Are the proposals in the Draft Bill at s 89 and following adequate to deal with the range of intrusions that are possible? Are you concerned about the current lack of an associated draft Code of Practice?

27. In the absence of a draft Code of Practice it is difficult for Parliament to assess the extent to which the interference permitted is proportionate to the legitimate need. The Bar Council has already identified in its earlier submission concerns that the Bill contains no express protection for material which is subject to legal professional privilege (LPP), and no process by which such access would be identified. Such a failure is not proportionate, and it is doubtful whether inclusion of protection for LPP material in a Code of Practice would suffice, in particular if it mirrors the current draft RIPA Code which allows targeted interception of LPP communications. Unless Parliament can be satisfied that the Bill itself contains provisions which ensure that warrants will be proportionate to legitimate security or investigative needs, the burden will be placed on Judicial Commissioners to interpret what they think Parliament must have intended.

Bar Council
21st December 2015

Ian Batten—written evidence (IPB0090)

1. I am Ian Batten, now a lecturer in computer security at the University of Birmingham. I was formerly Head of Information Assurance at Fujitsu Telecommunications Europe, in which role I amongst other things was responsible for security and lawful interception facilities in Fujitsu's DSLAM and MSAN products. These products still form a substantial portion of the broadband infrastructure of the UK. I now teach network security and networking technology; in this I draw on my thirty years' experience with implementing and securing networks and services using the Internet's TCP/IP protocol suite.

2. I am writing to address the Communications Data and Data Retention sections of the consultation.

3. Internet Connection Records are described on p.25 of the draft bill, in the explanatory material. They are however defined for legislative purposes in S.47(6) of the draft bill. For reference, the wording is:

In this section "internet connection record" means data which—

(a) may be used to identify a telecommunications service to which a communication is transmitted through a telecommunication system for the purpose of obtaining access to, or running, a computer file or computer program, and

(b) is generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication (whether or not a person).

4. Data is transmitted over the Internet in the form of packets. To take the example of the transmission of a file (perhaps a photograph or video), it is split into units of approximately 1500 bytes, which are sent from sender to recipient. A photograph might be perhaps one thousand such packets; a film could be several million.

5. Each packet is numbered. It is the responsibility of the receiver to reassemble the file from the packets it receives, and to request the retransmission of any that have either gone astray or been damaged in transit. It is as though a book were to be sent by putting each page in a separate envelope, and the receiver checks they have all the pages and uses the page numbers to request fresh copies of any that are missing or illegible.

6. It is, however, no concern of the Internet Service Provider as to whether any individual packet forms part of a photograph, or a book, or something entirely different. It is also no concern of the ISP as to whether a particular packet is part of one file or another.

7. This is because the Internet's core protocol suite, commonly called TCP/IP consists of what is known as a stack of protocols. Each protocol draws on the services of protocols lower down the stack, and provides services to those above it.

Application protocols, such as HTTP and FTP, used for specific purposes, use…
…Transport protocols such as TCP, which provide reliable transfer of data and rely on…

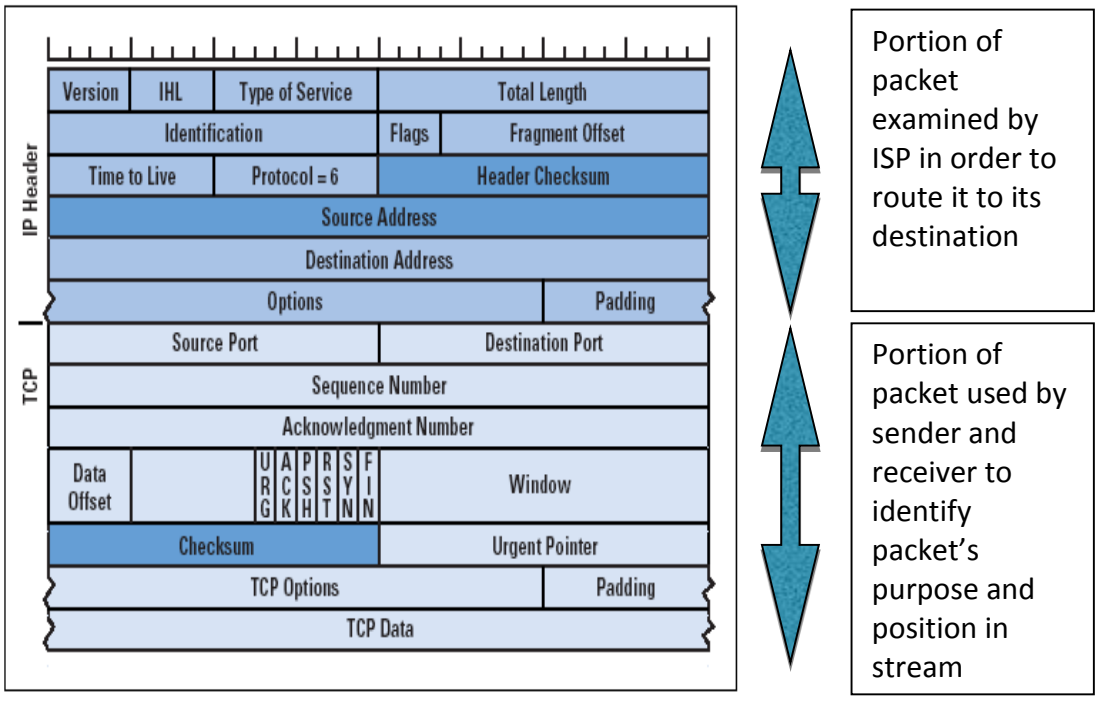
…Network protocols such as IP, which allow units of data to be moved between systems and rely on…
…Link layer protocols such as Ethernet which allow data to be moved between adjacent computers

8. Typically, files (and other forms of bulk data such as streaming video) are transmitted using a protocol called TCP, the Transmission Control Protocol. On the sending side, this provides a standard mechanism for the process of splitting a stream of data into packets, numbering them, marking them as being a part of one stream and not any other stream, and handing them to a lower layer to be transmitted. The receiver then follows the reverse process by taking the packets from a lower layer, putting the packets back into sequence and give them to the appropriate application.

9. The lower layer in this case is IP, the Internet Protocol. In paragraph 5 I used the analogy of the individual numbered pages of a book each being placed in an envelope. IP cannot see the page numbers, or indeed whether or not the envelopes contain pages at all: it simply looks at the address on the front of the envelope and routes the packet to its destination.

10. In physical terms each protocol is encapsulated by the protocol below it. HTTP, used by web browsers, is placed into TCP packets, which are in turn placed inside IP packets, which are in turn placed inside (often) Ethernet packets (known, for historical reasons, as

Figure 1: TCP/IP Header Fields Altered by NATs (Outgoing Packet)



frames).

11. So a particular packet will usually consist of an ethernet header, used to route the packet locally between machines on the same physical network, followed by an IP header, used to route the packet over the Internet more widely, followed by a TCP header, which is

of significance only to the sender and the receiver, followed by the application data used by your web browser or Smart TV.

12. From the perspective of TCP, each packet contains a numbered part of a stream of data, together with indications as to which stream it belongs.

13. However, from the perspective of IP, it is just a packet, whose contents are of no concern to the IP layer.

14. The core equipment used by ISPs does not necessarily understand TCP, and frequently can only deal with the TCP protocol by taking packets out of the fast, hardware-accelerated routing path and processing them with far slower software. All that is required by a core router for an ISP is that it processes IP, as quickly as possible. The reassembly of a sequence of IP packets into a TCP connection is carried out only by the receiving system: there is no requirement that the individual packets of that stream are sent in order, or even down only one path.

15. Specialised equipment can be used to examine streams of data and to reassemble TCP streams. This is required for some forms of network management and debugging, when the equipment is known generically as an analyser. It is also required for a range of security applications, when the equipment is known as a firewall (amongst other names). Such equipment can identify, amongst other things, the start and end of a particular stream of data, and can between those end points associate packets with particular streams.

16. However, returning to S.47(6)(b) of the draft bill, the requirement for Internet Connection Records is that the data used should be "generated or processed by a telecommunications operator in the process of supplying the telecommunications service"

17. But the TCP header, which I suspect is what is intended to be referred to here, is categorically **not** processed or generated by the telecommunications service. The telecommunications service need only look at the IP header. The IP header does not provide sufficient information to identify particular streams.

18. Millions of IP frames are generated per day per user. In the past fortnight, my home network — which is not used for NetFlix or other high-volume services — has transmitted 118 million packets and received 80 million packets, or a total of approximately 14 million per day.

19. In the absence of TCP information to group connections together, the "Internet Connection Records" would require that information about every such packet be logged. This is clearly infeasible. From what is known in the open community, GCHQ's TEMPORA project, with the resources of a major national state, is only able to capture and log a small fraction of the UK's Internet traffic and do so for only a few days.

20. However, the obvious discriminator to use to group packets together into individual flows of data, whose logging might be more practical, requires (a) that the equipment in use by the ISP is able to perform this, which in many cases it either cannot or cannot at suitable speeds and (b) that the equipment examines the TCP header in order to determine the packet's purpose. ISPs do not routinely use firewalls or other equipment in their network to

examine customer packets, therefore S.47(6)(b) fails: the use of the TCP header is not covered by the current draft legislation.

21. Moving on from this point, we can consider the utility of this data. A common example which is invoked to justify ICRs is the missing child who might have been using Facebook from their smart phone. Let us leave aside the point that rather than examining the metadata of their Internet usage, a reasonable starting position is "yes, a teenager uses Facebook". But more seriously, their phone will at most show that yes, at various points over the past few days, it has connected to Facebook. What is the utility of this? Parents and friends will rapidly be able to confirm this, and the ICRs will not show anything about what was communicated or to whom.

22. On the other hand, anyone who wishes conceal their activities will have no difficulty in doing so and may in fact find it has been concealed in advance. There are any number of services, entirely legal services with legitimate purposes, whose effect would be to make all of the packets leaving the subject's network appear to be going to destinations other than the final one. Some would be used at the behest of the subscriber, some at the behest of the service provider, some at the behest of the final target service. As well as the obvious TOR whose sole purpose is this obfuscation, there are the VPNs used to secure remote working, content delivery networks used to accelerate downloading and many more.

23. Consider, for example, the Cloudflare service. This interposes itself between users and web sites, providing protection against denial of service attacks and also accelerating the delivery of content. They claim to have two million websites under their protection; the ICR for access to any of these would be indistinguishable from access to any other. The same applies to other content delivery networks such as Akamai. It would I suspect only be a matter of time before law enforcement grew tired of the ICRs being useless, and started to ask for yet more invasive analysis of traffic to attempt to discern the ultimate destination; this would be met by a rising level of encryption, and the arms race would continue.

24. To summarise:

A. S.47(6) as written prevents the examination of flows of data, which would be necessary to gain any utility at reasonable cost from ICRs'

B. There are many ways in which careful users can conceal their activities;

C. There are many ways in which entirely benign features of the Internet will obscure the contents anyway.

21 December 2015

BCS, The Chartered Institute for IT—written evidence (IPB0075)

BCS, The Chartered Institute for IT

BCS is a charity with a Royal Charter. Its mission is to make IT better for society. It does this through leadership on societal and professional issues, working with communities and promoting excellence.

BCS brings together industry, academics, practitioners, educators and government to share knowledge, promote new thinking, educate, shape public policy and inform the public. This is achieved through and with a network of 75,000 members across the UK and internationally. BCS is funded through membership fees, through the delivery of a range of professional development tools for practitioners and employers, and as a leading IT qualification body, through a range of widely recognised professional and end-user qualifications.

www.bcs.org

Executive Summary

Introduction

1. The draft Bill has generated significant debate within BCS in attempting to reconcile intrusive powers and mass surveillance with the needs of the police and intelligence agencies to gain targeted access to information as part of their investigations. While the Home Office's assurance that the Bill will be compatible with the European Convention on Human Rights, the content of the draft Bill has raised concerns about the impact on privacy.

Thematic questions

Are the powers sought necessary? BCS believes the draft Bill has substantially developed the argument for the new powers and for the restating and clarifying existing powers. BCS particularly welcomes the consolidation of existing powers and oversight within a common regulatory structure. However, BCS believes that more is required to clarify necessity and proportionality to secure the trust of society.

2. **Are the powers sought legal?** BCS believes the proposed powers are compatible with Article 8 of both the Human Rights Act 1998 and the ECHR. However, there appear to be some inconsistencies with the draft Bill and the Data Protection Act 1998 that need to be resolved. The public seek the assurance of the law in protecting their privacy by ensuring that its use is proportionate and only enabled within robust legal safeguards and visible and effective oversight.

Are the powers sought workable and carefully defined? BCS believes that the draft Bill adequately explain the types of activity that could be undertaken under these powers.

However, the rapid advance in communications technology together with the manner of its exploitation make it difficult to predict future threats and countermeasures. The manner in which these powers are employed should be monitored and periodically reviewed to ensure they remain necessary and fit for purpose.

3. **Are the powers sought sufficiently supervised?** BCS believes the authorisation process to be appropriate if properly resourced. BCS understands that the cross-party Intelligence and Security Committee of Parliament (ISC) will be ultimately responsible for oversight which has the ability to monitor use and directly challenge Commissioners, oversight bodies, the security and intelligence services and law enforcement bodies as necessary and that any member of the public can bring a complaint directly to the Investigatory Powers Tribunal (IPT) regarding the use of these powers which the we commend.

Specific Question

4. **General -** A number of Bills have been introduced or amended in recent years in response to the growing cybercrime/terrorist threat and the emergence of new technology. BCS believes the draft Bill to be a major review of existing surveillance powers and obligations pertaining to communications service provision. The draft Bill clarifies the different roles of the of the security and intelligence services and law enforcement, introducing a unified judicial authorisation process with appropriate oversite. BCS believes the new offences proposed in the draft Bill are necessary and the penalties appropriate to enable the law to effectively address the threat to society.

Interception - BCS believes political and judicial authorisation to be a significant step forward. However, greater clarification is required on the role of judicial commissioners for the Home Secretary's statement suggests that the role of judicial commission will be to make decisions on judicial review principles, not on the basis of evidence, while BCS believe that the judiciary should review interception requests based on evidence. International collaboration is generally best achieved basis based on mutual trust and shared interest. While the introduction of the draft Bill presents an opportunity for the UK to be seen as taking a lead in the fight against cybercrime and terrorism there will be many who see it as an attack on civil liberties; the problem is in achieving the right balance. While consensus on the right balance between security and privacy remains unresolved an internationally accepted solution to this issue remains elusive.

5. **Communication Data -** BCS believes the terms employed and the process proposed by the draft Bill to capture and where necessary share communication data with the appropriate organisations, and people within those organisations to be well defined and workable.

6. **Data Retention -** BCS believes the authorisation regime and safeguards for bulk data retention proposed by the draft Bill go some way to addressing the concerns raised by the two legal challenges. However, BCS believes that the principles of necessity and proportionality need to be more prominent in the presentation of the argument for change to address the legitimate concerns of the individual in protecting their privacy.

7. **Equipment Interference -** BCS believes that in the interests of national security a credible argument can be made for the security and intelligence services to undertake both targeted and bulk equipment interference. However, if law enforcement was allowed direct access to such powers it may necessitate disclosure of what software was used to carry out interference in subsequent legal proceedings. While this may be resisted, it would otherwise undermine any digital forensic evidence.

8. **Bulk Personal Data -** BCS recognises the need for the use of bulk personal datasets by the security and intelligence services in undertaking their legitimate surveillance role on behalf of national security. However, given the significant harm that unlawful access to sensitive data would bring, it is relevant not only to target those who abuse access, but also those who fail to properly manage security risks by including 'reckless' disclosure as well as acquisition as a criminal offence.

9. **Oversight -** BCS believes the creation of a single Judicial Commission to oversee the use of investigatory powers is sensible way forward. A single commission can overcome the potential conflicts of jurisdiction, enable greater clarity and visibility while ensuring improved coordination. However, to ensure these benefits are realised the new commission must be properly resourced. Otherwise the advantages will be lost, response times will suffer, the process will not secure the confidence of practitioners and a case backlog develop rendering the IPC unable to discharge its statutory responsibilities. The key factor in determining the effectiveness of the review and appeals process is the impartiality of the Tribunal and the transparency of the review mechanism for seeking redress in the event of abuse or wrong doing.

1. Introduction

1.1 The draft Bill has generated significant debate within BCS in attempting to reconcile intrusive powers and mass surveillance with the needs of the police and intelligence agencies to gain targeted access to information as part of their investigations. While the Home Office's assurance that the Bill will be compatible with the European Convention on Human Rights, the content of the draft Bill has raised concerns about the impact on privacy.

1.2 BCS recognises the progress that has been made in addressing this issue over a number of years, and in particular the improved public engagement on the topic from the Home Office and security services. BCS also recognise that this is a major harmonisation of a disparate set of existing powers; a difficult and thankless task. BCS welcomes and supports these initiatives and the progress achieved. There are, however, issues that remain worth highlighting below.

Consultation Overarching/thematic questions:

2. Are the powers sought necessary?

2.1 Has the case been made, both for the new powers and for the restated and clarified existing powers?

2.1.1 BCS has observed the 'intercept modernisation' process which culminated in the production of the draft Bill. BCS previous critiques have focused on three key areas; public debate, proportionality and governance/oversight. BCS believes the present draft Bill has made major steps forward in addressing these concerns.

2.1.2 BCS accepts the need for the state to engage in digital surveillance within the terms of European Convention on Human Rights (ECHR) provided it is proportionate and enabled only within robust legal safeguards and visible and effective oversight.

2.1.3 BCS believes the draft Bill has substantially developed the argument for the new powers and for the restating and clarifying existing powers. BCS particularly welcomes the consolidation of existing powers and oversight within a common regulatory structure. However, BCS believes that more is required to clarify necessity and proportionality to secure the trust of society.

3. Are the powers sought legal?

3.1 Are the powers compatible with the Human Rights Act and the ECHR?

3.1.1 BCS believes that the proposed powers are compatible with both the Human Rights Act 1998 and the ECHR. Common to both is the wording of Article 8, the 'right to respect for private and family life', Section 2 states that *'There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'*

3.1.2 However BCS believes that there are some inconsistencies with the new offences proposed by the draft Bill and the Data Protection Act 1998, see 6.3.2, and inconsistencies with the Court of Justice of the European Union (CJEU) and it judgement on the legality of the Data Retention Directive (DRD), see 9.1.

3.1.3 Article 8 is considered to be one of the ECHR's most open-ended provisions. Implicit in acceptance of this flexibility citizens seek the assurance of the law in protecting their privacy by ensuring that its use is proportionate and only enabled within robust legal safeguards and visible and effective oversight.

3.2 Is the requirement that they be exercised only when necessary and proportionate fully addressed?

3.2.1 There is little doubt that public opinion remains sanguine about the proportionality of mass data capture and intrusion. Similarly, there is little doubt that amongst technical communities there is a level of worry about these measures far in excess of the feeling of the public. It is difficult to say what is responsible for this gap, but one concern is that the technical community are better able to conceptually understand the scale and implications of what is being proposed. Proportionality ultimately is a political matter that BCS will not seek to define, but we would raise a cautionary note that as society experiences the outworking of this Bill the public mood may shift.

3.2.2 BCS believes necessity and proportionality to be key aspect of the argument for change that have not been adequately addressed in the draft Bill. While relevant in a number or different areas these two aspects which deliver comfort and assurance are neither specifically addressed or quantified. A short section emphasising relevance, qualifying the terms and supported by a short case study demonstrating appropriate use would be beneficial.

3.3 Are they sufficiently clear and accessible on the face of the draft Bill?

3.3.1 The face of the draft Bill makes a constructive attempt at rendering the context understandable by the general public. It is fundamentally challenging to explain the technological environment that is hidden from view, conflated with difficulty about the covert nature of the activities it describes. The scale and power of what is being described is a sensitive matter, and that could be treated in a more forthright manner.

3.4 Is the legal framework such that CSPs (especially those based abroad) will be persuaded to comply?

3.4.1 BCS believes that securing the cooperation and compliance of CSPs will be a major challenge. The need for CSPs to store data for twelve months and to provide wider assistance to law enforcement organisations will increase operating costs and the cost of compliance will ultimately fall to their UK customers, either directly as consumers or indirectly through the government underwriting the costs of service providers. Many CSPs operate internationally and the need to coexist in different legislative regimes will prove unpopular to CSPs and customers may decide to take their business elsewhere.

3.4.2 Implementation of Data Retention Directive EC/24/2006 was not well received by CPSs and the recent decision by the Court of Justice of the European Union which declared the Directive to be invalid will not aid the introduction of new regulatory measures.

3.4.3 The legal framework proposed for CSPs owned and operating within the UK can be made to work but the reaction of CSPs based outside UK jurisdiction is more difficult to predict for they will assess the cost, and risk, of compliance against the

value of their UK business. Business advantage will undoubtedly be the key motivator in gaining compliance, and a 'kite mark' government approval scheme should be considered.

3.4.4 While many other nations are considering similar legislation a co-ordinated approach leading to internationally accepted standard will be difficult to achieve in the short term.

3.5 Are concerns around accessing journalists', legally privileged and MPs' communications sufficiently addressed?

3.5.1 BCS believes that concerns around accessing journalists', legally privileged and MPs' communications have been sufficiently addressed. The Codes of Practice and added levels of authorisation appear to provide the additional levels of protection necessary in these more sensitive areas.

4. Are the powers sought workable and carefully defined?

4.1 Are the technological definitions accurate and meaningful (e.g. content vs communications data, internet connection records etc.)?

4.1.1 BCS believes the technological definitions employed in the draft bill are accurate and meaningful at this time. The Cabinet Office maintain an online Glossary of Terms, https://data.gov.uk/glossary, developed to assist in the drafting data and information technology related documents.

4.2 Does the draft Bill adequately explain the types of activity that could be undertaken under these powers?

4.2.1 BCS believes that the draft Bill adequately explain the types of activity that could be undertaken under these powers. However, the rapid advance in communications technology together with the manner of its exploitation makes it difficult to predict future threats and the countermeasures necessary. The manner in which these powers are employed should be monitored and periodically reviewed to ensure they remain necessary and fit for purpose.

4.3 Is the wording of the powers sustainable in the light of rapidly evolving technologies and user behaviours?

4.3.1 BCS believes that the present wording of the powers is suitable, but the nature of changing technology and social interaction across technology makes this inherently challenging. This should not prevent the draft Bill from progressing, and the wording is suitable as far as can be predicted.

4.4 **Overall is the Bill future-proofed as it stands?**

4.4.1 BCS believes the overall the Bill to be future-proofed as it stands for at least the next five years, while recognising the inherent unpredictability of the environment.

5. Are the powers sought sufficiently supervised?

5.1 Is the authorisation process appropriate?

5.1.1 BCS believes the authorisation process for the various investigative task is appropriate. In any operational environment requiring formal authorisation the process needs to be adequately resourced to ensure that operational risk due to delay is minimised.

5.2 Will the oversight bodies be able adequately to scrutinise their operation?

5.2.1 BCS believes that if properly staffed and resourced the oversight bodies proposed will be able to adequately monitor and scrutinise their operation.

5.3 What ability will Parliament and the public have to check and raise concerns about the use of these powers?

5.3.1 BCS understands that the cross-party Intelligence and Security Committee of Parliament (ISC) will be ultimately responsible for oversight which has the ability to monitor use of these powers and directly challenge Commissioners, oversight bodies, the security and intelligence services and law enforcement bodies as necessary. Any member of the public can bring a complaint directly to the Investigatory Powers Tribunal (IPT) regarding the use of these powers.

Consultation Specific questions:

6. General

6.1 To what extent is it necessary for (a) the security and intelligence services and (b) law enforcement to have access to investigatory powers such as those contained in the Draft Investigatory Powers Bill?

6.1.1 BCS believes that in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others it is necessary for the security and intelligence services for law enforcement agencies to have access to investigatory powers such as those contained in the draft Bill within robust legal safeguards and visible and effective oversight.

6.1.2 In recent years the progressive rise in cybercrime and international terrorism have resulted in an increase in the demands of security and intelligence services and

law enforcement agencies for greater surveillance and investigatory powers together with the increased cooperation of communications providers to combat this increased threat to society.

6.1.3 A number of Bills have been introduced or amended in recent years in response to this growing cybercrime/terrorist threat and the emergence of new technology. BCS believes the draft Bill represents a major review of the framework in respect of existing surveillance powers and obligations pertaining to communications service provision. The draft Bill identifies the different roles of the of the security and intelligence services and law enforcement agencies, introducing a unified judicial authorisation process with appropriate oversite.

6.2 Are there any additional investigatory powers that security and intelligence services or law enforcement agencies should have which are not included in the draft Bill?

6.2.1 BCS believes the powers contained within the draft Bill address the essential requirements of the security and intelligence services and law enforcement agencies as understood at this time.

6.3 Are the new offences proposed in the draft Bill necessary?

6.3.1 BCS believes that with the dramatic increase in cybercrime and international terrorism the new offences proposed in the draft Bill are necessary to enable law enforcement to effectively address the threat to society.

6.3.2 However, BCS is concerned that the draft Bill proposes to introduce a new criminal offence, which a communications provider would commit in disclosing to the subject of a communications data acquisition notice the existence of that notice (Clause 66). This would appear to be contra to the Data Protection Act 1998, which provides that "the subject information provisions shall have effect notwithstanding any enactment or rule of law prohibiting or restricting the disclosure, or authorising the withholding, of information". This conflict will need to be resolved.

6.4 Are the suggested punishments appropriate?

6.4.1 BCS believes the suggested punishments to be in line with present UK legal and judicial practice and appropriate. The draft Bill offers a range of penalties enabling a mix of custodial sentences together with a fine which may be adjusted to fit the impact and severity of the offence.

6.4.2 While the draft Bill is worded in terms of the individual offender wrong doing is frequently the result of corporate behaviour or policy. Provision should be available to enable the prosecution of a corporate entity and/or the Directors of that entity where the magnitude of any financial penalty is substantially greater commensurate with the magnitude of the damage caused.

7. Interception

7.1 Are the proposed authorisation processes for such interception activities appropriate?

7.1.1 BCS believe political and judicial authorisation to be a significant step forward, however greater clarification is required on the role of judicial commissioners. Whilst the Home Secretary's statement was very encouraging the bill itself suggests that the role of judicial commission will be to make decisions on judicial review principles, not on the basis of evidence. BCS believe that the judiciary should review interception requests based on evidence.

7.2 Is the proposed process for authorising urgent warrants workable?

7.2.1 Authorising urgent warrants in a 24/7 operational environment is always a problem and a source of concern to both law enforcement practitioners and the public to ensure that action is within the law. BCS believes the proposed process for authorising urgent warrants in the draft Bill is workable, but believe that it should be subject to periodic review to ensure that it remains fit for purpose.

7.3 Are the proposed safeguards sufficient for the secure retention of material obtained from interception?

7.3.1 BCS believes that the safeguards proposed in the draft Bill, if fully implemented, to be sufficient for the secure retention of material obtained from interception within UK jurisdiction. This will require the close cooperation and collaboration of all service providers engaged in the interception process.

7.4 How well does the current process under Mutual Legal Assistance Treaties (MLATs) work for the acquisition of communications data?

7.4.1 Cooperation with between foreign security and intelligence services and law enforcement agencies is generally best achieved on a bi-lateral basis based on mutual trust and shared interest. Engagement with foreign based communications data companies generally requires the active support and assistance of the host country to enable access and/or sharing of locally hosted data.

7.4.2 In the absence of such bi-lateral agreements or if the enquiry is not directly from the security and intelligence services and law enforcement agencies the MLAT can be employed but this may take some time and may not prove successful. There is presently a considerable backlog for general information requests to the UK under this scheme.

7.4.3 BCS believes that with the introduction of the new Bill additional work is required in enhancing co-operation with communication data service suppliers and key hosting nations to agree and improve legal access to essential data and to foster wider international agreement and best practice in this area.

7.5 What will be the effect of the extra-territorial application of the provisions on communications data in the draft Bill?

7.5.1 BCS believes the extra-territorial application of the provisions on communications data in the draft Bill will be difficult to judge. While many advanced economies recognise the threat and risks they share have been slow to move in the introduction of similar legislation. Others have introduced legislation have faced challenges in the courts, widening public debate. While consensus on the right balance between security and privacy remains unresolved an internationally accepted solution to this issue remains elusive.

7.5.2 The introduction of the draft Bill presents an opportunity for the UK to be seen as taking a lead in the fight against cybercrime and terrorism there will be many who see it as an attack on civil liberties; the problem is in achieving the right balance.

8. Communications Data

8.1 Are the definitions of content and communications data (including the distinction between 'entities' and 'events') sufficiently clear and practical for the purposes of accessing such data?

8.1.1 BCS believes the definitions of content and communications data (including the distinction between 'entities' and 'events') sufficiently clear and practical for the purposes of accessing such data. The Cabinet Office maintain an online Glossary of Terms, https://data.gov.uk/glossary, developed to assist in the drafting data and information technology related documents, which may be of assistance.

8.2 Does the draft Bill allow the appropriate organisations, and people within those organisations, access to communications data?

8.2.1 BCS believes the process proposed by the draft Bill to capture and where necessary share communication data with the appropriate organisations, and people within those organisations to be defined and workable.

8.3 Are there sufficient operational justifications for accessing communications data in bulk?

8.3.1 BCS understands the operational and technical for need accessing communications data in bulk and believes that the draft Bill presents a sufficiently robust argument to justify its operational use within robust legal safeguards and effective oversight.

8.4 Is the authorisation process for accessing communications data appropriate?

8.4.1 BCS believes the authorisation process proposed for accessing communications data to be rigours and appropriate. The principle of single point of

contact enables the authorised sharing of communication data to be more visible ensuring effective and rigorous oversight.

9. Data Retention

9.1 Do the proposed authorisation regime and safeguards for bulk data retention meet the requirements set out in the CJEU Digital Rights Ireland and the Court of Appeal Davis judgments?

9.1.1 The EU Data Retention Directive provisions the retention of certain data generated or processed by providers of publicly available electronic communication services and the use of that data for the prevention, investigation, detection and prosecution of serious crime and terrorism. CJEU has declared the DRD to be invalid. CJEU believes DRD interferes in a particularly serious manner with the fundamental rights to respect for private life and the protection of personal data. CJEU is of the opinion that by adopting the DRD the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality.

9.1.2 Similarly the High Court found that sections 1 and 2 of Data Retention and Investigatory Powers Act 2014 (DRIPA) breached the public's rights to protection of personal data and to respect for private life and communications under the EU Charter of Fundamental Rights because, they fail to provide clear and precise rules to ensure data is accessed only for preventing, detecting or prosecuting serious crime and they do not require data to be authorised by a court or independent body, which could limit access to and use of data to what is strictly necessary.

9.1.3 BCS believes the authorisation regime and safeguards for bulk data retention proposed by the draft Bill do appear to go some way to addressing the concerns raised by these two legal challenges. However, BCS believes that the principles of necessity and proportionality need to be more prominent in the presentation of the argument for change to address the legitimate concerns of the individual in protecting their privacy.

9.1.4 BCS has received expressions of concern from some of our membership that Internet Service Providers (ISP) are only able to retain incoming emails and therefore some individuals may be victim to intrusion of Human Rights Act 1998, Article 8 rights on the basis that they have been victim to receiving communications which they had not been the intended recipient.

9.2 Is accessing Internet Connection Records (ICR) essential for the purposes of IP resolution and identifying of persons of interest?

9.2.1 BCS believes that accessing ICR is essential for identifying the sender of an online communication, identifying which ISP is being used and where and when illegal content has been accessed. While not ideal as only partial connection data is recovered as the full web addressed is defined as content, and content may not be

viewed. This information can be crucial in identifying of persons of interest and/or providing evidence of wrong doing.

9.3 Are there alternative mechanisms?

9.3.1 BCS understands there may be alternative mechanism which would be more intrusive, involve higher levels of co-ordination and greater co-operation of Internet ISPs and additional operational costs. However, striking the right balance between protecting society from wrong doers and protecting the privacy of the individual should be the prime consideration ensuring a necessary and proportional response.

9.4 Are the proposed safeguards on accessing Internet Connection Records data appropriate?

9.4.1 BCS believes that the safeguards on accessing ICR data are appropriate. However, while the stored data records exist there is always a risk that unscrupulous individuals will seek to benefit from their existence. Safeguards must ensure that the likelihood of detection is high and the penalty to ISP and individual is heavy.

9.5 Are the requirements placed on service providers necessary and feasible?

9.5.1 BCS believes the requirements placed on service providers are necessary to enable the ICR data to be stored and used by the security and intelligence services. The requirements are feasible but only with the active participation and co-operation of the ISP at a cost which is ultimately recovered from the ISP's customers.

9.5.2 The imposition of a retention order on an ISP is likely to require the reconfiguration of their network and the generation and storage of additional data to comply with the order. This was a contentious aspect of the draft Communications Data Bill which generated much adverse criticism from ISPs.

10. Equipment Interference

10.1 Should the security and intelligence services have access to powers to undertake (a) targeted and (b) bulk equipment interference?

10.1.1 BCS believes that in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others a credible argument can be made for the security and intelligence services to undertake both targeted and bulk equipment interference.

10.2 Should law enforcement also have access to such powers?

10.2.1 BCS believes that if law enforcement was allowed access to such powers it may necessitate disclosure of what software was used to carry out interference in subsequent legal proceedings. While this may be resisted, it would otherwise

undermine any digital forensic evidence, and provides a new source of what is known as the Trojan Horse defence. That is where software is run on a device, and the function of that software is not disclosed, anything can be claimed to have been an "interference" and hence reduce the value of any digital evidence by providing reasonable doubt. Since this type of evidence is used in the majority of a cases to some extent, it will be a self-defeating proposition.

10.3 Are the authorisation processes for such equipment interference activities appropriate?

10.3.1 While BCS considers the authorisation processes for such equipment interference activities to be appropriate, the principles of necessity and proportionality should always be seen to be applied.

10.4 Are the safeguards for such activities sufficient?

10.4.1 BCS considers the safeguards for such activities proposed in the draft Bill if properly resourced to be sufficient.

11. Bulk Personal Data

11.1 Is the use of bulk personal datasets by the security and intelligence services appropriate?

11.1.1 BCS recognises the tactical need for gaining access to, and the use of bulk personal datasets by the security and intelligence services in undertaking their legitimate surveillance role on behalf of national security and the detection of wrong doing. BCS believes that the use of bulk personal datasets is justified only in pursuit of objectives and only within strict judicial authorisation and supervision.

11.1.2 BCS understands that currently bulk personal data retained by the security and intelligence services under DRIPA is subject to Data Protection Act 1998, under which the data must be protected by the National Data Protection Authority (ICO) and as such is subject to disclosure, such disclosure should be subject to judicial authorisation.

11.2 Are the safeguards sufficient for the retention and access of potentially highly sensitive data?

11.2.1 BCS believes the safeguards proposed in the draft Bill to be sufficient for the retention and access of potentially highly sensitive data to be adequate provided they are properly resourced and monitored.

11.2.2 BCS believes that given the significant harm that unlawful access to sensitive data would bring, it is relevant not only to target those who abuse access, but also those who fail to properly implement systems in ways that manage security risks. By covering 'reckless' disclosure as well as acquisition, the criminal offence would

extend to anyone who is designing or implementing the system in a manner that would be professionally reckless. This would place responsibility and a need for proper process on those designing and implementing the systems and support public confidence while technical implementations cannot be publicly disclosed / scrutinised. Consider amending the wording of the new criminal offence in the draft Bill to include reckless disclosure of data, thus creating a criminal liability for anyone who egregiously fails to use good practice in systems design, implementation and operation.

12. Oversight

12.1 What are the advantages and disadvantages of the proposed creation of a single Judicial Commission to oversee the use of investigatory powers?

12.1.1 BCS believes the creation of a single Judicial Commission to oversee the use of investigatory powers is sensible way forward. A single commission can overcome the potential conflicts of jurisdiction, enable greater clarity and visibility while ensuring improved coordination. However, to ensure these benefits are realised the new commission must be properly resourced. Otherwise the advantages will be lost, response times will suffer, the process will not secure the confidence of practitioners and a case backlog develop rendering the IPC unable to discharge its statutory responsibilities.

12.2 Would the proposed Judicial Commission have sufficient powers, resources and independence to perform its role satisfactorily?

12.2.1 BCS agrees with the necessity of acting quickly, but is concerned that the constraints on judicial oversight limit its utility for a useful judicial review should cover more than simply a process check and give public confidence that activities are lawful. This requires an evidence check if it is to achieve the desired public confidence in the process implied by judicial oversight. To facilitate this the IPC must be independently resourced with skilled assessors and adjudicators capable of evaluating the evidence and passing a balanced judgement on the lawful nature of activities.

12.3 Are the appointment and accountability arrangements for Judicial Commissioners appropriate?

12.3.1 BCS consider the appointment and accountability arrangements for Judicial Commissioners described in the draft Bill to be appropriate.

12.4 Are the new arrangements for the Investigatory Powers Tribunal including the possibility of appeal adequate or are further changes necessary?

12.4.1 BCS consider the new arrangements for the Investigatory Powers Tribunal including the possibility of appeal to be adequate. The key factor in determining the effectiveness of the review and appeals process is the impartiality of the Tribunal

and the transparency of the review mechanism for seeking redress in the event of abuse or wrong doing.

21 December 2015

Dr Paul Bernal—supplementary written evidence (IPB0018)

I am making this submission in my capacity as Lecturer in Information Technology, Intellectual Property and Media Law at the UEA Law School. I research in internet law and specialise in internet privacy from both a theoretical and a practical perspective. My PhD thesis, completed at the LSE, looked into the impact that deficiencies in data privacy can have on our individual autonomy, and set out a possible rights-based approach to internet privacy. My book, *Internet Privacy Rights – Rights to Protect Autonomy*, was published by Cambridge University Press in 2014. I am a member of the National Police Chiefs' Council's *Independent Digital Ethics Panel*. The draft Investigatory Powers Bill therefore lies precisely within my academic field.

I gave oral evidence to the Committee on 7th December 2015: this written evidence is intended to expand on and explain some of the evidence that I gave on that date. If any further explanation is required, I would be happy to provide it.

One page summary of the submission

The submission looks specifically at the nature of internet surveillance, as set out in the Bill, at its impact on broad areas of our lives – not just what is conventionally called 'communications' – and on a broad range of human rights – not just privacy but freedom of expression, of association and assembly, and of protection from discrimination. It looks very specifically at the idea of 'Internet Connection Records, briefly at data definitions and at encryption, as well as looking at how the Bill might be 'future proofed' more effectively.

The submission will suggest that in its current form, in terms of the overarching/thematic questions set out in the Committee's Call for Written Evidence, it is hard to conclude that all of the powers sought are **necessary**, uncertain that they are **legal**, likely that many of them are neither **workable** nor **carefully defined,** and unclear whether they are sufficiently **supervised**. In some particular areas – Internet Connection Records is the example that I focus on in this submission – the supervision envisaged does not seem sufficient or appropriate. Moreover, there are critical issues – for example the vulnerability of gathered data – that are not addressed at all. These problems potentially leave the Bill open to successful legal challenge and rather than 'future-proofing' the Bill, they provide what might be described as hostages to fortune.

Many of the problems, in my opinion, could be avoided by taking a number of key steps. Firstly, rethinking (and possibly abandoning) the Internet Connection Records plans. Secondly, being more precise and open about the Bulk Powers, including a proper setting out of examples so that the Committee can make an appropriate judgment as to their proportionality and to reduce the likelihood of their being subject to legal challenge. Thirdly, taking a new look at encryption and being clear about the approach to end-to-end encryption. Fourthly, strengthening and broadening the scope of oversight. Fifthly, through the use of some form of renewal or sunset clauses to ensure that the powers are subject to full review and reflection on a regular basis.

1 Introductory remarks

1.1 Before dealing with the substance of the Bill, there is an overriding question that needs to be answered: why is the Committee being asked to follow such a tight timetable? This is a critically important piece of legislation – laws concerning surveillance and interception are not put forward often, particularly as they are long and complex and deal with highly technical issues. That makes detailed and careful scrutiny absolutely crucial. Andrew Parker of MI5 called for 'mature debate' on surveillance immediately prior to the introduction of the Bill: the timescale set out for the scrutiny of the Bill does not appear to give an adequate opportunity for that mature debate.

1.2 Moreover, it is equally important that the debate be an accurate one, and engaged upon with understanding and clarity. In the few weeks since the Bill was introduced the public debate has been far from this. As shall be discussed below, for example, the analogies chosen for some of the powers envisaged in the Bill have been very misleading. In particular, to suggest that the proposed 'Internet Connection Records' ('ICRs') are like an 'itemised phone bill', as the Home Secretary described it, is wholly inappropriate. As I set out below (in section 5) the reality is very different. There are two possible interpretations for the use of such inappropriate analogies: either the people using them don't understand the implications of the powers, which means more discussion is needed to disabuse them of their illusions, or they are intentionally oversimplifying and misleading, which raises even more concerns.

1.3 For this reason, the first and most important point that I believe the Committee should be making in relation to the scrutiny of the Bill is that more time is needed. As I set out below (in 8.4 below) the case for the urgency of the Bill, particularly in the light of the recent attacks in Paris, has not been made: in many ways the attacks in Paris should make Parliament pause and reflect more carefully about the best approach to investigatory powers in relation to terrorism.

1.4 In its current form, in terms of the overarching/thematic questions set out in the Committee's Call for Written Evidence, it is hard to conclude that all of the powers sought are **necessary**, uncertain that they are **legal**, likely that many of them are neither **workable** nor **carefully defined,** and unclear whether they are sufficiently **supervised**. In some particular areas – Internet Connection Records is the example that I focus on in this submission – the supervision envisaged does not seem sufficient or appropriate. Moreover, there are critical issues – for example the vulnerability of gathered data – that are not addressed at all. These problems potentially leave the Bill open to successful legal challenge and rather than 'future-proofing' the Bill, they provide what might be described as hostages to fortune.

1.5 Many of the problems, in my opinion, could be avoided by taking a number of key steps. Firstly, rethinking (and possibly abandoning) the Internet Connection Records plans. Secondly, being more precise and open about the Bulk Powers, including a proper setting out of examples so that the Committee can make an appropriate judgment as to their proportionality and to reduce the likelihood of their being subject to legal challenge. Thirdly, taking a new look at encryption and being clear about the approach to end-to-end encryption. Fourthly, strengthening and broadening the scope of oversight. Fifthly, through the use of some form of renewal or sunset clauses to ensure that the powers are subject to full review and reflection on a regular basis.

2 The scope and nature of this submission

2.1 This submission deals specifically with the gathering, use and retention of communications data, and of Internet Connection Records in particular. It deals more closely with *the internet* rather than other forms of communication – this is my particular area of expertise, and it is becoming more and more important as a form of communications. The submission does not address areas such as Equipment Interference, and deals only briefly with other issues such as interception and oversight. Many of the issues identified with the gathering, use and retention of communications data, however, have a broader application to the approach adopted by the Bill.

2.2 It should be noted, in particular, that this submission does not suggest that it is unnecessary for either the security and intelligence services or law enforcement to have investigatory powers such as those contained in the draft Bill. Many of the powers in the draft Bill are clearly critical for both security and intelligence services and law enforcement to do their jobs. Rather, this submission suggests that as it is currently drafted the bill includes some powers that are poorly defined, poorly suited to the stated function, have more serious repercussions than seem to have been understood, and could represent a distraction, a waste of resources and add an unnecessary set of additional risks to an already risky environment for the very people that the security and intelligence services and law enforcement are charged with protecting.

3 The Internet, Internet Surveillance and Communications Data

3.1 The internet has changed the way that people communicate in many radical ways. More than that, however, it has changed the way people live their lives. This is perhaps the single most important thing to understand about the internet: we do not just use it for what we have traditionally thought of as 'communications', but in almost every aspect of our lives. We don't just talk to our friends online, or just do our professional work online, we do *almost everything* online. We bank online. We shop online. We research online. We find relationships online. We listen to music and watch TV and movies online. We plan our holidays online. We try to find out about our health problems online. We look at our finance online. For most people in our modern society, it is hard to find a single aspect of our lives that does not have a significant online element.

3.2 This means that internet interception and surveillance has a far bigger potential impact than traditional communications interception and surveillance might have had. Intercepting internet communications is not the equivalent of tapping a telephone line or examining the outside of letters sent and received, primarily because we use the internet for far more than we ever used telephones or letters. This point cannot be overemphasised: the uses of the internet are growing all the time and show no signs of slowing down. Indeed, more dimensions of internet use are emerging all the time: the so-called 'internet of things' which integrates 'real world' items (from cars and fridges to Barbie dolls[105]) into the internet is just one example.

3.3 This is also one of the reasons that likening Internet Connection Records to an itemised phone bill is particularly misleading. Another equally important reason to challenge

[105] The new 'Hello Barbie' doll, through which a Barbie Doll can converse and communicate with a child, has caused some controversy recently (see for example http://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children but is only one of a growing trend.

that metaphor is the nature and potential uses of the data itself. What is labelled Communications Data (and in particular 'relevant communications data', as set out in clause 71(9) of the draft Bill) is by nature of its digital form ideal for analysis and profiling. Indeed, using this kind of data for profiling is the heart of the business models of Google, Facebook and the entire internet advertising industry.

3.4 The inferences that can be – and are – drawn from this kind of data, through automated, algorithmic analysis rather than through informed, human scrutiny – are enormous and are central to the kind of 'behavioural targeting' that are the current mode of choice for internet advertisers. Academic studies have shown that very detailed inferences can be drawn: analysis of Facebook 'Likes', for example, has been used to indicate the most personal of data including sexuality, intelligence and so forth. A recent study at Cambridge University concluded that 'by mining Facebook Likes, the computer model was able to predict a person's personality more accurately than most of their friends and family.'[106]

3.5 This means that the kind of 'communications' data discussed in the Bill is vastly more significant that what is traditionally considered to be communications. It also means that from a human rights perspective more rights are engaged by its gathering, holding and use. Internet 'communications' data does not just engage Article 8 in its 'correspondence' aspect, but in its 'private and family life' aspect. It engages Article 10 – the impact of internet surveillance on freedom of speech has become a bigger and bigger issue in recent years, as noted in depth by the UN Special Rapporteur on Freedom of Expression, most recently in his report on encryption and anonymity.[107]

3.6 Article 11, which governs Freedom of Association and Assembly, is also critically engaged: not only do people now associate and assemble online, but they use online tools to organise and coordinate 'real world' association and assembly. Indeed, using surveillance to perform what might loosely be called chilling for association and assembly has become one of the key tools of the more authoritarian governments to stifle dissent. Monitoring and even shutting off access to social media systems, for example, was used by many of the repressive regimes in the Arab Spring. Even in the UK, the government communications plan for 2013/14 included the monitoring of social media in order to 'head off badger cull protests', as the BBC reported.[108] This kind of monitoring does not necessarily engage Article 8, as Tweets (the most obvious example to monitor) are public, but it would engage both aspects of Article 11, and indeed of Article 10.

3.7 Article 14, the prohibition of discrimination, is also engaged: the kind of profiling discussed in paragraph 3.4 above can be used to attempt to determine a person's race, gender, possible disability, religion, political views, even direct information like membership of a trade union. It should be noted, as is the case for all these profiling systems, that accuracy is far from guaranteed, giving rise to a bigger range of risks. Where derived or profiling data is accurate, it can involve invasions of privacy, chilling of speech and discrimination: where it is inaccurate it can generate injustice, inappropriate decisions and further chills and discrimination.

---

[106] See http://www.cam.ac.uk/research/news/computers-using-digital-footprints-are-better-judges-of-personality-than-friends-and-family#sthash.OSQ8dqdr.dpuf

[107] Available online at http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx

[108] http://www.bbc.co.uk/news/uk-politics-22984367

3.8 This broad range of human rights engaged means that the 'proportionality bar' for any gathering of this data, interception and so forth is higher than it would be if only the correspondence aspect of Article 8 were engaged. It is important to understand that the underlying reason for this is that privacy is not an individual, 'selfish', right, but one that underpins the way that our communities function. We need privacy to communicate, to express ourselves, to associate with those we choose, to assemble when and where we wish – indeed to do all those things that humans, as social creatures, need to do. Privacy is a collective right that needs to be considered in those terms.

3.9 It is also critical to note that communications data is not 'less' intrusive than content: it is 'differently' intrusive. In some ways, as has been historically evident, it is less intrusive – which is why historically it has been granted lower levels of protection – but increasingly the intrusion possible through the gathering of communications data is in other was greater than that possible through examination of content. There are a number of connected reasons for this. Firstly, it is more suitable for aggregation and analysis – communications data is in a structured form, and the volumes gathered make it possible to use 'big data' analysis, as noted above. Secondly, content can be disguised more easily – either by technical encryption or by using 'coded' language. Thirdly, there are many kinds of subjects that are often avoided deliberately when writing content – things like sexuality, health and religion – that can be determined by analysis of communications data. That means that the intrusive nature of communications data can often be greater than that of content. Moreover, as the levels and nature of data gathered grows, the possible intrusions are themselves growing. This means that the idea that communications data needs a lower level of control, and less scrutiny, than content data is not really appropriate – and in the future will become even less appropriate.

4 When rights are engaged

4.1 A key issue in relation to the gathering and retention of communications data is when the relevant rights are engaged: it is when data is gathered and retained, when it is subject to algorithmic analysis or automated filtering, or when it is subject to human examination. When looked at from what might be viewed an 'old fashioned' communications perspective, it is only when humans examine the data that 'surveillance' occurs and privacy is engaged. In relation to internet communications data this is to fundamentally miss the nature of the data and the nature of the risks. In practice, many of the most important risks occur at the gathering stage, and more at what might loosely be described as the 'automated analysis' stage.

4.2 It is fundamental to the nature of data that when it is gathered it becomes vulnerable. This vulnerability has a number of angles. There is vulnerability to loss – from human error to human malice, from insiders and whistle-blowers to hackers of various forms. The recent hacks of Talk Talk and Ashley Madison in particular should have focussed the minds of any envisaging asking communications providers to hold more and more sensitive data. There is vulnerability to what is variously called 'function creep' or 'mission creep': data gathered for one reason may end up being used for another reason. Indeed, when business models of companies such as Facebook and Google are concerned this is one of the key features: they gather data with the knowledge that this data is useful and that the uses will develop and grow with time.

4.3 It is also at the gathering stage that the chilling effects come in. The Panopticon, devised by Bentham and further theorised about by Foucault, was intended to work by encouraging 'good' behaviour in prisoners through the possibility of their being observed, not by the actual observation. Similarly it is the knowledge that data is being gathered that chills freedom of expression, freedom of association and assembly and so forth, not the specific human examination of that data. This is not only a theoretical analysis but one borne out in practice, which is one of the reasons that the UN Special Rapporteur on Freedom of Expression and many others have made the link between privacy and freedom of expression.[109]

4.4 Further vulnerabilities arise at the automated analysis stage: decisions are made *by* the algorithms, particular in regard to filtering based on automated profiling. In the business context, services are tailored to individuals automatically based on this kind of filtering – Google, for example, has been providing automatically and personally tailored search results to all individuals since 2009, without the involvement of humans at any stage. Whether security and intelligence services or law enforcement use this kind of a method is not clear, but it would be rational for them to do so: this does mean, however, that more risks are involved and that more controls and oversight are needed at this level as well as at the point that human examination takes place.

4.5 Different kinds of risks arise at each stage. It is not necessarily true that the risks are greater at the final, human examination stage. They are qualitatively different, and engage different rights and involve different issues. If anything, however, it is likely that as technology advances the risks at the earlier stages – the gathering and then the automated analysis stages – will become more important than the human examination stage. It is critical, therefore, that the Bill ensures that appropriate oversight and controls are put in place at these earlier stages. At present, this does not appear to be the case. Indeed, the essence of the data retention provisions appears to be that no real risk is considered by the 'mere' retention of data. That is to fundamentally misunderstand the impact of the gathering of internet communications data.

5 Internet Connection Records

5.1 Internet Connection Records ('ICRs') have been described as the only really new power in the Bill, and yet they are deeply problematic in a number of ways. The first is the question of definition. The 'Context' section of the Guide to Powers and Safeguards (the Guide) in the introduction to the Bill says that:

> "The draft Bill will make provision for the retention of internet connection records (ICRs) in order for law enforcement to identify the communications service to which a device has connected. This will restore capabilities that have been lost as a result of changes in the way people communicate." (paragraph 3)

This is further explained in paragraphs 44 and 45 of the Guide as follows:

> "44. A kind of communications data, an ICR is a record of the internet services a specific device has connected to, such as a website or instant messaging application. It is captured by the company providing access to the internet. Where available, this

[109] See for example the 2015 report of the UN Special Rapporteur on Freedom of Expression, where amongst other things he makes particular reference to encryption and anonymity. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement

> data may be acquired from CSPs by law enforcement and the security and intelligence agencies.
>
> 45. An ICR is not a person's full internet browsing history. It is a record of the services that they have connected to, which can provide vital investigative leads. It would not reveal every web page that they visit or anything that they do on that web page."

Various briefings to the press have suggested that in the context of web browsing this would mean that the URL up to the first slash would be gathered (e.g. www.bbc.co.uk and not any further e.g. http://www.bbc.co.uk/sport/live/football/34706510). On this basis it seems reasonable to assume that in relation to app-based access to the internet via smartphones or tablets the ICR would include the activation of the app, but nothing further.

5.2 The 'definition' of ICRs in the bill is set out in 47(6) as follows:

> "In this section "internet connection record" means data which—
>
> (a) may be used to identify a telecommunications service to which a communication is transmitted through a telecommunication system for
>
> the purpose of obtaining access to, or running, a computer file or computer program, and
>
> (b) is generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication (whether or not a person)."

This definition is vague, and press briefings have suggested that the details would be in some ways negotiated directly with the communications services. This does not seem satisfactory at all, particularly for something considered to be such a major part of the Bill: indeed, the only really new power according to the Guide. More precision should be provided within the Bill itself – and specific examples spelled out in Codes of Practice that accompany the Bill, covering the major categories of communications envisaged. Initial versions of these Codes of Practice should be available to Parliament at the same time as the Bill makes its passage through the Houses.

5.3 The Bill describes the functions to which ICRs may be put. In 47(4) it is set out that ICRs (and data obtained through the processing of ICRs) can only be used to identify:

> "(a) which person or apparatus is using an internet service where—
>
> (i) the service and time of use are already known, but
>
> (ii) the identity of the person or apparatus using the service is not known,
>
> (b) which internet communications service is being used, and when and how it is being used, by a person or apparatus whose identity is already known, or
>
> (c) where or when a person or apparatus whose identity is already known is obtaining access to, or running, a computer file or computer program which wholly or mainly involves making available, or acquiring, material whose possession is a crime."

The problem is that in all three cases ICRs insofar as they are currently defined are very poorly suited to performing any of these three functions – and better methods either

already exist for them or could be devised to do so. ICRs provide at the same time much more information (and more intrusion) than is necessary and less information than is adequate to perform the function. In part this is because of the way that the internet is used and in part because of the way that ICRs are set out. Examples in the following paragraphs can illustrate some (but not all) of the problems.

5.4 The intrusion issue arises from the nature of internet use, as described in Section 3 of this submission. ICRs cannot be accurately likened to 'itemised telephone bills'. They do not record the details of who a person is communicating with (as an itemised telephone bill would) but they do include vastly more information, and more sensitive and personal information, than an itemised telephone bill could possibly contain. A record of websites visited, even at the basic level, can reveal some of the most intimate information about an individual – and not in terms of what might traditionally be called 'communications'. This intrusion could be direct – such as accessing a website such as www.samaritans.org at 3am or accessing information services about HIV – or could come from profiling possibilities. The commercial profilers, using what is often described as 'big data' analysis (and has been explained briefly in section 3 above) are able to draw inferences from very few pieces of information. Tastes, politics, sexuality, and so forth can be inferred from this data, with a relatively good chance of success.

5.5 This makes ICRs ideal for profiling and potentially subject to function-creep/mission-creep. It also makes them ideally suited for crimes such as identity theft and personalised scamming, and the databases of ICRs created by communications service providers a perfect target for hackers and malicious insiders. By gathering ICRs, a new range of vulnerabilities are created. Data, however held and whoever it is held by, is vulnerable in a wide range of ways.[110] Recent events have highlighted this very directly: the hacking of Talk Talk, precisely the sort of provider who would be expected to gather and store ICRs, should be taken very seriously. Currently it appears as though this hack was not done by the kind of 'cyber-terrorists' that were originally suggested, but by disparate teenagers around the UK. Databases of ICRs would seem highly likely to attract the interest both hackers of many different kinds. In practice, too, precisely those organisations who should have the greatest expertise and the greatest motivations to keep data secure – from the MOD and HMRC and the US DoD to Swiss Banks, technology companies including Sony and Apple – have all proved vulnerable to hacking or other forms of data loss in recent years. Hacking is the most dramatic, but human error, human malice, collusion and corruption, and commercial pressures (both to reduce costs and to 'monetise' data) may be more significant – and the ways that all these vulnerabilities can combine makes the risk even more significant.

5.6 ICRs are also unlikely to provide the information that law enforcement and the intelligence and security services need in order to perform the three functions noted above. The first example of this is Facebook. Facebook messages and more open communications would seem on the surface to be exactly the kind of information that law enforcement might need to locate missing children – the kind of example referred to in the introduction and guide to the bill. ICRs, however, would give almost no relevant information in respect of Facebook. In practice, Facebook is used in many different ways by many different people – but the general approach is to remain connected to Facebook all the time. Often this will

[110] Some of the potential range of vulnerabilities are discussed in Chapter 6 of my book Internet Privacy Rights – Rights to Protect Autonomy, Cambridge University Press, 2014.

literally be 24 hours a day, as devices are rarely turned off at night – the 'connection' event has little relationship to the use of the service. If Facebook is accessed by smartphone or tablet, it will generally be via an app that runs in the background at all times – this is crucial for the user to be able to receive notifications of events, of messages, of all kinds of things. If Facebook is accessed by PC, it may be by an app (with the same issues) or through the web – but if via the web this will often be using 'tabbed browsing' with one tab on the browser keeping the connection to Facebook available without the need to reconnect.

5.7 Facebook and others encourage and support this kind of long-term and even permanent connection to their services – it supports their business model and in a legal sense gives them some kind of consent to the kind of tracking and information gathering about their users that is the key to their success. ICRs would not help in relation to Facebook except in very, very rare circumstances. Further, most information remains available on Facebook in other ways. Much of it is public and searchable anyway. Facebook does not delete information except in extraordinary circumstances – the requirement for communications providers to maintain ICRs would add nothing to what Facebook retains.

5.8 The story is similar in relation to Twitter and similar services. A 24/7 connection is possible and indeed encouraged. Tweets are 'public' and available at all times, as well as being searchable and subject to possible data mining. Again, ICRs would add nothing to the ways that law enforcement and the intelligence and security services could use Twitter data. Almost all the current and developing communications services – from WhatsApp and SnapChat to Pinterest and more – have similar approaches and ICRs would be similarly unhelpful.

5.9 Further, the information gathered through ICRs would fail to capture a significant amount of the 'communications' that can and do happen on the internet – because the interactive nature of the internet now means that almost any form of website can be used for communication without that communication being the primary purpose of the website. Detailed conversations, for example, can and do happen on the comments sections of newspaper websites: if an analysis of ICRs showed access to www.telegraph.co.uk would the immediate thought be that communications are going on? Similarly, coded (rather than encrypted) messages can be put on product reviews on www.amazon.co.uk. I have had detailed political conversations on the message-boards of the 'Internet Movies Database' (www.imdb.com) but an ICR would neither reveal nor suggest the possibility of this.

5.10 This means that neither can the innocent missing child be found by ICRs via Facebook or its equivalents nor can the even slightly careful criminal or terrorist be located or tracked. Not enough information is revealed to find either – whilst extra information is gathered that adds to intrusion and vulnerability. The third function stated for ICRs refers to people *whose identity is already known*. For these people, ICRs provide insufficient information to help. This is one of the examples where more targeted powers would help – and are already envisaged elsewhere in the Bill.

5.11 The conclusion for all of this is that ICRs are not likely to be a useful tool in terms of the functions presented. The closest equivalent form of surveillance used around the world has been in Denmark, with very poor results. In their evaluation of five years' experience the Danish Justice Ministry concluded that 'session logging', their equivalent of Internet

Connection Records, had been of almost no use to the police.[111] It should be noted that when the Danish 'session logging' suggestion was first made, the Danish ISPs repeatedly warned that the system would not work and that the data would be of little use. Their warnings were not heeded. Similar warnings from ISPs in the UK have already begun to emerge. The argument has been made that the Danish failure was a result of the specific technical implementation – I would urge the Committee to examine it in depth to come to a conclusion. However, the fundamental issues as noted above are only likely to grow as the technology becomes more complex, the data more dense and interlinked, and the use of it more nuanced. All these trends are likely only to increase in speed.

5.12 The gathering and holding of ICRs are also likely to add vulnerabilities to all those about whom they are collected, as well as requiring massive amounts of data storage at a considerable cost. At a time when resources are naturally very tight, for the money, expertise and focus to be on something like this appears inappropriate.

6 Other brief observations about communications data, definitions and encryption

6.1 There is still confusion between 'content' and 'communications' data. The references to 'meaning' in 82(4), 82(8),106(8) and 136(4) and emphasised in 193(6) seem to add rather than reduce confusion – particularly when considered in relation to the kinds of profiling possible from the analysis of basic communications data. It is possible to derive 'meaning' from almost any data – this is one of the fundamental problems with the idea that content and communications can be simply and meaningfully separated. In practice, this is far from the case.[112] Further, Internet Connection Records are just one of many examples of 'communications' data that can be used to derive deeply personal information – and sometimes more directly (through analysis) than often confusing and coded (rather than encrypted) content.

6.2 There are other issues with the definitions of data – experts have been attempting to analyse them in detail in the short time since the Bill was published, and the fact that these experts have been unable to agree or at times even ascertain the meaning of some of the definitions is something that should be taken seriously. Again it emphasises the importance of having sufficient time to scrutinise the Bill. Graham Smith of Bird & Bird, in his submission to the Commons Science and Technology Committee,[113] notes that the terms 'internet service' and 'internet communications service' used in 47(4) are neither defined nor differentiated, as well as a number of other areas in which there appears to be significant doubt as to what does and does not count as 'relevant communications data' for retention purposes. One definition in the Bill particularly stands out: in 195(1) it is stated that *'"data" includes any information which is not data'*. Quite what is intended by this definition remains unclear.

6.3 In his report, 'A question of trust', David Anderson QC called for a law that would be 'comprehensive and comprehensible': the problems surrounding definitions and the lack of

[111] See http://www.ft.dk/samling/20121/almdel/reu/bilag/125/1200765.pdf - in Danish
[112] This has been a major discussion point amongst legal academics for a long time. See for example the work of Daniel Solove, e.g. Reconstructing Electronic Surveillance Law, Geo. Wash. L. Review, vol 72, 2003-2004
[113] Published on the Committee website at http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25119.pdf

clarity about the separation of content and communications data mean that the Bill, as drafted, does not meet either of these targets yet. There are other issues that make this failure even more apparent. The lack of clarity over encryption – effectively leaving the coverage of encryption to RIPA rather than drafting new terms – has already caused a significant reaction in the internet industry. Whether or not the law would allow end-to-end encryption services such as Apple's iMessage to continue in their current form, where Apple would not be able to decrypt messages themselves, needs to be spelled out clearly, directly and comprehensibly. In the current draft of the Bill it does not.

6.4 This could be solved relatively simply by the modification of 189 'Maintenance of technical capability', and in particular 189(4)(c) to make it clear that the Secretary of State cannot impose an obligation to remove electronic protection that is a basic part of the service operated, and that the Bill does not require telecommunications services to be designed in such a way as to allow for the removal of electronic protection.

7 Future Proofing the Bill

7.1 One of the most important things for the Committee to consider is how well shaped the Bill is for future developments, and how the Bill might be protected from potential legal challenges. At present, there are a number of barriers to this, but there are ways forward that could provide this kind of protection.

7.2 The first of these relates to ICRs, as noted in section 5 above. The idea behind the gathering ICRs appears on the face of it to be based upon an already out-dated understanding of both the technology of the internet and of the way that people use it. In its current form, the idea of requiring communications providers to retain ICRs is also a hostage to fortune. The kind of data required is likely to become more complex, of a vastly greater volume and increasingly difficult to use. What is already an unconvincing case will become even less convincing as time passes. The best approach would seem to be to abandon the idea of requiring the collection of ICRs entirely, and looking for a different way forward.

7.3 Further, ICRs represent one of the two main ways in which the Bill appears to be vulnerable to legal challenge. It is important to understand that recent cases at both the CJEU (in particular the Digital Ireland case[114] and the Schrems case[115]) and the European Court of Human Rights (in particular the Zakharov case[116]) it is not just the examination of data that is considered to bring Article 8 privacy rights into play, but the gathering and holding of data. This is not a perverse trend, but rather a demonstration that the European courts are recognising some of the issues discussed above about the potential intrusion of gathering and holding data. It is a trend that is likely to continue. Holding data of innocent people on an indiscriminate basis is likely to be considered disproportionate. That means that the idea of ICRs – where this kind of data would be required to be held – is very likely to be challenged in either of these courts and indeed is likely to be overturned at some point.

7.4 The same is likely to be true of the 'Bulk' powers, unless those bulk powers are more tightly and clearly defined, including the giving of examples. At the moment quite what

[114] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, April 2014, which resulted in the invalidation of the Data Retention Directive

[115] Case C-362/14, Maximillian Schrems v Data Protection Commissioner, October 2015, which resulted in the declaration of invalidity of the Safe Harbour agreement.

[116] Roman Zakharov v. Russia (application no. 47143/06), ECtHR, December 2015

these bulk powers consist of – and how 'bulky' they are – is largely a matter of speculation, and while that speculation continues, so does legal uncertainty. If the powers involve the gathering and holding of the data of innocent people on a significant scale, a legal challenge either now or in the future seems to be highly likely.

7.5 It is hard to predict future developments either in communications technology or in the way that people use it. This, too, is something that seems certain to continue – and it means that being prepared for those changes needs to be built into the Bill. At present, this is done at least in part by having relatively broad definitions in a number of places, to try to ensure that future technological changes can be 'covered' by the law. This approach has a number of weaknesses – most notably that it gives less certainty than is helpful, and that it makes 'function creep' or 'mission creep' more of a possibility. Nonetheless, it is probably inevitable to a degree. It can, however, be ameliorated in a number of ways.

7.6 The first of these ways is to have a regular review process built in. This could take the form of a 'sunset clause', or perhaps a 'renewal clause' that requires a new, full, debate by Parliament on a regular basis. The precise form of this could be determined by the drafters of the Bill, but the intention should be clear: to avoid the situation that we find ourselves in today with the complex and almost incomprehensible regime so actively criticised by David Anderson QC, RUSI and to an extent the ISC in their reviews.

7.7 Accompanying this, it is important to consider not only the changes in technology, but the changes in people's behaviour. One way to do this would be to charge those responsible for the oversight of communications with a specific remit to review how the powers are being used *in relation to* the current and developing uses of the internet. They should report on this aspect specifically.

8 Overall conclusions

8.1 I have outlined above a number of ways in which the Bill, in its current form, does not seem to be workable, proportionate, future-proofed and protected from potential legal challenges. I have made five specific recommendations:

8.1.1 I do not believe the case has been made for retaining ICRs. They appear unlikely to be of any real use to law enforcement in performing the functions that are set out, they add a significant range of risks and vulnerabilities, and are likely to end up being extremely expensive. This expense is likely to fall upon both the government – in which case it would be a waste of resources that could be put to more productive use to achieve the aims of the Bill – or ordinary internet users through increased connection costs.

8.1.2 The Bill needs to be more precise and open about the Bulk Powers, including a proper setting out of examples so that the Committee can make an appropriate judgment as to their proportionality and to reduce the likelihood of their being subject to legal challenge.

8.1.3 The Bill needs to be more precise about encryption and to be clear about the approach to *end-to-end* encryption. This is critical to building trust in the industry, and in particular with overseas companies such as those in Silicon Valley. It is also a way to future-proof the Bill: though some within the security and intelligence services may not like it, strong encryption is fundamental to the internet now and

will become even more significant in the future. This should be embraced rather than fought against.

8.1.4 Oversight needs strengthening and broadening – including oversight of how the powers have been used in relation to changes in behaviour as well as changes in technology

8.1.5 The use of some form of renewal or sunset clause should be considered, to ensure that the powers are subject to full review and reflection by parliemant on a regular basis.

8.2 The question of resource allocation is a critical one. For example, have alternatives to the idea of retaining ICRs been properly considered for both effectiveness and costs? The level of intrusion of internet surveillance (as discussed in section 3 above) adds to the imperative to consider other options. Where a practice is so intrusive, and impacts upon such a wide range of human rights (Articles 8, 10, 11 and 14 of the ECHR – and possibly Article 6), a very high bar has to be set to make it acceptable. It is not at all clear either that the height of that bar has been appropriately set or that the benefits of the Bill mean that it has met them. In particular, the likely ineffectiveness of ICRs mean that it is very hard to argue that this part of the Bill would meet even a far lower requirement. The risks and vulnerabilities that retention of ICRs adds will in all probability exceed the possible benefits, even without considering the intrusiveness of their collection, retention and use.

8.3 The most important overall conclusion at this stage, however, is that more debate and analysis is needed. The time made available for analysis is too short for any kind of certainty, and that means that the debate is being held without sufficient information or understanding. Time is also needed to enable MPs and Lords to gain a better understanding of how the internet works, how people use it in practice, and how this law and the surveillance envisaged under its auspices could impact upon that use. This is not a criticism of MPs or Lords so much as a recognition that people in general do not have that much understanding of how the internet works – one of the best things about the internet is that we can use it quickly and easily without having to understand much of what is actually happening 'underneath the bonnet' as it were. In passing laws with significant effects – and the Investigatory Powers Bill is a very significant Bill – much more understanding is needed.

8.4 It is important for the Committee not to be persuaded that an event like the recent one in Paris should be considered a reason to 'fast-track' the Bill, or to extend the powers provided by the Bill. In Paris, as in *all* the notable terrorism cases in recent years, from the murder of Lee Rigby and the Boston Bombings to the Sydney Café Siege and the Charlie Hebdo shootings, the perpetrators (or at the very least a significant number of the perpetrators) were already known to the authorities. The problem was not a lack of data or a lack of intelligence, but the use of that data and that intelligence. The issue of resources noted above applies very directly here: if more resources had been applied to 'conventional' intelligence it seems, on the surface at least, as though there would have been more chance of the events being avoided. Indeed, examples like Paris, if anything, argue against extending large-scale surveillance powers. If the data being gathered is already too great for it to be properly followed up, why would gathering more data help?

8.5 As a consequence of this, in my opinion the Committee should look not just at the detailed powers outlined in the Bill and their justification, but also more directly at the alternatives to the overall approach of the Bill. There are significant costs and

consequences, and the benefits of the approach as opposed to a different, more human-led approach, have not, at least in public, been proven. The question should be asked – and sufficient evidence provided to convince not just the Committee but the public and the critics in academia and elsewhere. David Anderson QC made 'A Question of Trust' the title of his review for a reason: gaining the trust of the public is a critical element here.

15 December 2015

Anam Bevardis—written evidence (IPB0100)

[01] The proposed Investigatory Powers Bill violates a core legal principle that has stood for centuries.

[02] Police cannot search your house without permission. They cannot, for example, search every house in a town to look for drugs, even though this would undoubtably catch criminals.

[03] But under the draft bill, police and intelligence can take a copy of all UK persons' private data, and have analysts with computers search that data prior to suspicion.

[04] It is well established in UK law that police and intelligence agencies cannot violate the privacy of communications without prior suspicion. In the case of technological surveillance such as wiretaps, a higher standard of a warrant signed by a magistrate is necessary.

[05] On the Internet, wiretaps and interception can now reveal much more private information. Not only voice communication, but photography and video, including explicit photography and video between partners, private data from smartphone apps, a person's calendar, address book, diary, financial records and so on. Even metadata, or data about data, referred to in the draft bill as communications data, can be analysed with today's advanced technology to reveal information in ways that would violate privacy.

[06] But this new draft bill authorises, for example, systems that would record communications of all UK citizens, including and especially those not suspected of any wrongdoing, and especially you, yourself, the person who reads this document now.

[07] It allows the recording, specifically, of communications in a situation where a person would have a reasonable expectation of privacy, and where such recording would not be authorised by a magistrate's warrant, probably cause, reasonable suspicion or even a passing suspicion. This entirely violates the principle of privacy, in the general case, rather than in cases of necessary exception.

[08] Such a law has already been challenged and repealed in the United States, and to apply such a law in the United Kingdom looking only at the optimistically imagined benefits, without balancing against the the clear and egregious privacy violations of all citizens, is a violation of all the basic freedoms our nation stands for.

21 December 2015

Krishan Bhasin—written evidence (IPB0034)

Are the powers sought necessary?
No coherent, logical or reasonable case has been made for the powers being sought in this bill.
It is clear that one of the main problems with the current intelligence system is that there is far too much data being taken in, and it is becoming more and more difficult to separate the useful signals from the background noise. With the volume of data that we as produce as a population growing exponentially or faster, it is quite simply impossible to expect there to be enough humans working to process it all, especially with the extra volume of data that this bill seeks to allow GHCQ to sift through.
France has very intrusive surveillance laws and found itself unable to prevent attacks in Paris, despite the attackers using unencrypted SMS', most of the perpetrators already being known to the intelligence services as potential threats, and several travelling to and from Syria.
This clearly indicates that in order to maintain the safety of the United Kingdom, the focus needs to shift back towards highly targeted surveillance, with the intelligence services using 'traditional' methods to locate potential threats before placing them under specific surveillance, after obtaining a warrant from an independent judge.

Furthermore, David Anderson QC has pointed out that Denmark tried collecting records similar to the "Internet Connection Records" that this bill calls for, and they abandoned it after finding it of no use to the police and intelligence services.

Are the powers legal?
These laws are fundamentally incompatible with the European Convention on Human Rights, specifically with Articles 5 and 8, the rights to liberty & security and to private & family life.
This point was very recently affirmed by the European Court of Human Rights, which ruled that 'blanket interception of communications' (which this bill also does en-mass) violated basic human rights.
In addition, this bill legalises the illegal activities that GCHQ have been carrying out for the past decade or longer – no effort is made to provide recourse over the previous breaches of the law.

Are the powers sought workable and carefully defined?
No.
The powers are extraordinarily ill-defined, using terms like "equipment interference" to reference hacking, and provide no clarity whatsoever on how they will be implemented. This is extremely dangerous, as it was revealed that the 1984 Telecommunications Act was being used to justify the bulk collection of telephone records, a use that was never conceived when it was being written; this was made possible by its vague wording. We must therefore ensure that ambiguous wording is avoided in this bill.

Are the powers sufficiently supervised?
No. One of the key requirements set out by the Anderson report (and others) for a mass surveillance system was that all data access was via a judicial warrant.

The government has claimed that this bill provides this judicial oversight, however when one looks into the detail it becomes extremely clear that this is merely in the capability of a 'rubber stamp' with judges unable to oppose requests on the basis of their proportionality and reason, instead left only to check if proper process has been followed.

Are there sufficient operational justifications for undertaking (a) targeted and (b) bulk interception?

There are clear operational justifications for undertaking targeted surveillance of those suspected of committing, or those who are deemed highly likely to commit serious crimes, as long as the actions undertaken are deemed reasonable and proportional by an independent judge.

There is no clear, coherent or reasonable case for bulk interception of data, be it of citizens of the United Kingdom, or otherwise. The justifications provided for bulk collection were clearly demonstrated to be extremely flawed by Adrian Kennard, and can be found here: http://www.me.uk/IPBill-evidence1.pdf

It summarises that the "Internet Connection Records" would be largely useless due to the nature of modern communications; most apps are communicating continuously with their servers simply by virtue of being installed on a device, meaning that the intelligence services & police force will be unable to identify which ones had been used.

In addition, this 'honeypot' of citizen's data would be an extremely tempting dataset for malicious actors to attempt to obtain. If obtained, they could be used for blackmail & coercion, for ascertaining when properties are empty in order to target home thefts, among other things.

In summary, bulk interception provides at best a negligible increase in the government's capacity to protect against terrorism, and more likely actively harms this capability, while also seriously undermining civil liberties in the United Kingdom.

Is the use of bulk personal datasets by the security and intelligence services appropriate? Are the safeguards sufficient for the retention and access of potentially highly sensitive data?

No. To use an analogy, the intelligence services are searching for a very few needles in a large haystack. We have seen evidence that this is not working, and simply adding more hay to the pile will not make their tasks easier, and will not make attacks easier to stop.

17 December 2015

Big Brother Watch—written evidence (DIP0007)

About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaign group founded in 2009. We produce unique research which exposes the erosion of civil liberties in the UK, looks at the dramatic expansion of surveillance powers, the growth of the database state and the misuse of personal information.

Specific to this process we campaigned against the Data Retention and Investigatory Powers Act 2014 and gave both written and oral evidence to the Joint Committee on the draft Communications Data Bill. We have also called for the reform of RIPA for a number of years.

Key Points

- **The 'double-lock' system is not judicial authorisation and needs more work.**
- **A proper system of redress needs to be implemented to help protect citizens from unlawful surveillance.**
- **Encryption must be protected.**

Summary

This response will focus on ten areas which we believe need further scrutiny before any further Bill is published:

1. Judicial Authorisation
2. Communications Data
3. Internet Connection Records
4. Bulk Powers
5. Equipment Interference
6. Encryption
7. The Commissioner System
8. Interception
9. Redress/User Notification
10. Terminology

Initially we would like to raise concern about the time given for scrutiny, in particular the time given to the Joint Committee. By our estimation, excluding the period when the two Houses are not sitting, the Committee will have had only seven weeks to scrutinise the draft Bill, a document which runs to 296 pages and rewrites a key part of the surveillance capabilities of a number of Government bodies. When you compare this with the five months given to the Joint Committee for the draft Communications Data Bill for scrutiny of a 118 page document it is clear that the promise of full scrutiny given by the Government is, at best, lacking.[117]

Response

Judicial Authorisation

When the draft Investigatory Powers Bill was published the Home Secretary promised "*stringent safeguards and robust oversight, including 'double-lock' authorisation*" claiming that this would establish a "*world-leading oversight*" regime.[118] However the system which

[117] *Draft Communications Data Bill*, June 2012: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228824/8359.pdf

[118] T. May, *Home Secretary introduces draft Investigatory Powers Bill*, 4th November 2015: https://www.gov.uk/government/news/home-secretary-introduces-draft-investigatory-powers-bill

has been put forward to ensure the intrusive powers are used properly, is anything but world leading.

The much vaunted 'double-lock' authorisation system, which the Home Secretary claims would see "*the most intrusive powers*" subject to "*approval by a judge as well as by the Secretary of State*" does not, on reading of the draft Bill, provide a double lock, rather a process of "review" from a politically appointed Judicial Commissioner. Without a proper system of authorisation and oversight there can be no confidence that any of the powers will be used proportionately.[119]

In the past a wide range of individuals and organisations, for example the Joint Committee on Human Rights[120], the House of Lords Constitution Committee[121], General Michael Hayden, former Director of both the CIA and NSA[122] and the Chair of the Intelligence and Security Committee Rt. Hon Dominic Grieve MP[123], have called for an end to the ministerial authorisation of warrants and the introduction of judicial authorisation, their arguments have been based on the following:

1. The practicalities of a Secretary of State spending large amounts of time scrutinising warrants.

2. That no Secretary of State has ever explained their actions in relation to a warrant before Parliament, posing the question of strength of democratic accountability.
3. That independent judicial authorisation would harmonise us with other nations and would encourage service providers to work more closely with the agencies.

The proposed "double lock" system of political authorisation with judicial review fails to address any of these concerns.

Under **Sub-Clause 19(1)**, of the draft Bill it states that *"In deciding whether to approve a person's decision to issue a warrant under this Chapter, a Judicial Commissioner must review the person's conclusions as to the following matters".*

By asking the Judicial Commission to approve an existing decision using a method of review, relegates the Judicial Commissioner to little more than a rubber stamp, not the much vaunted "double lock".

The lack of power of the Judicial Commissioners is further emphasised at **Sub-Clause 19(5)** *"Where a Judicial Commissioner, other than the Investigatory Power Commissioner, refuses to approve a decision to issue a warrant... the person who made that decision may ask the Investigatory Powers Commissioner to decide whether to approve the decision to issue the warrant."*

---

[119] Ibid: https://www.gov.uk/government/news/home-secretary-introduces-draft-investigatory-powers-bill

[120] Joint Committee on Human Rights, Counter-Terrorism Policy and Human Rights: 28 days, intercept and post-charge questioning, September 2007, p. 9: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/243174/7215.pdf

[121] House of Lords Committee on the Constitution, Surveillance: Citizens and the state, 6th February 2009, p. 39: http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/18.pdf

[122] M. Hayden, Edward Snowden: Spies and the Law, 5th October 2015: http://www.bbc.co.uk/iplayer/episode/b06h7j3b/panorama-edward-snowden-spies-and-the-law

[123] D. Grieve, HC Deb, 25 June 2015, c1092, 25th June 2015: http://www.publications.parliament.uk/pa/cm201516/cmhansrd/cm150625/debtext/150625-0002.htm#150625-0002.htm_spnew140

Concerns about the proposed "double lock" have been raised by the Shadow Home Secretary, Rt Hon. Andy Burnham MP who wrote to the Home Secretary raising his concerns and the former Shadow Home Secretary Rt Hon. David Davis MP.[124] [125]
Effectively maintaining the current system with an extra process of review, does little to address the problems the warrantry process currently faces.
Secretaries of State will, under these proposals, continue to play a major role in scrutinising warrants. A process which may be simply unsustainable particularly when you consider that in 2014 alone the Home Secretary signed off 2,345 interception warrants, equivalent to 6 every day.[126]
The demand on time has been referred to be the **former Home Secretary, David Blunkett**:

> "*My whole world was collapsing around me. I was under the most horrendous pressure. I was barely sleeping, and yet I was being asked to sign government warrants in the middle of the night. My physical and emotional health had cracked*."[127]

Martin Chamberlain QC has pointed out that the combination of the large number of warrants and the varied responsibilities of a Secretary of State are not suited to providing proper scrutiny;

> "*The idea that the decision maker can apply her mind properly to every one of these* [warrants] *is far-fetched*".[128]

In an age when we must all have a digital presence to exist. With society becoming increasingly dominated by technology and data and with the Internet of Things beginning to encroach on all our lives; the sheer wealth of data which will be produced will be staggering. The impact this will have on the warrantry process should be explored further, as the proposed system may be creating an obligation which a Secretary of State will struggle to maintain.
Unless there is a re-evaluation of these proposals there is a real risk that the general public will have little faith that full, proper, independent safeguards will be in place to keep them safe.

Internet Connection Records

Internet Connection Records (ICRs) are the one new power in the draft Bill. They are defined on the Home Office factsheet as being "*records of the internet services that have been accessed by a device*" but which "*do not reveal every web page that a person has visited or any action carried out on that webpage.*"
The Home Secretary has stated that this data is "*the internet equivalent of a phone bill*";[129] however this is not entirely accurate. A telephone bill reveals who you have been speaking

---

[124] Guardian, *Andy Burnham calls for more judicial safeguards in the UK surveillance bill*, 9th November 2015: http://www.theguardian.com/politics/2015/nov/09/andy-burnham-investigatory-powers-bill-judicial-safeguards-letter-theresa-may
[125] Financial Times, *UK government's missed chance to fix broken surveillance system*, 6th November 2015: http://www.ft.com/cms/s/0/c7594530-83d6-11e5-8e80-1574112844fd.html#axzz3tA89DpBK
[126] D. Anderson, *A Question of Trust: Report of the Investigatory Powers Review*, p. 131, 11th June, 2015: https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf
[127] Guardian, *Blunkett: how I cracked under the strain of scandal*, 7th October 2006: http://www.theguardian.com/politics/2006/oct/07/uk.davidblunkett
[128] Guardian, *Specialist judges should oversee snooping warrants, says leading warrants*, 19th October 2015: http://www.theguardian.com/world/2015/oct/19/leading-lawyer-calls-specialist-judges-oversee-snooping-warrants
[129] Home Office, *Home Secretary introduces draft Investigatory Powers Bill*, 4th November 2015: https://www.gov.uk/government/news/home-secretary-introduces-draft-investigatory-powers-bill

to, when and for how long. Your internet activity on the other hand reveals every single thing you do online.

Analysing our internet history or what sites we have visited can provide a rich source of extremely revealing data which can be used to profile or create assumptions about an individual's life, connections and behaviour.

This is not the first time retention of this kind of data has been proposed. The draft Communications Data Bill proposed the retention of weblogs.[130] The Joint Committee who scrutinised that draft Bill determined that such proposals would creating a "*honeypot for casual hackers, blackmailers, criminals large and small from around the world and foreign states*"[131].

In their final report the same Joint Committee noted that:

> "*storing web log data, however securely, carries the possible risk that it may be hacked into or may fall accidentally into the wrong hands, and that, if this were to happen, potentially damaging inferences about people's interests or activities could be drawn.*"[132]

In light of this, if the Government wants the power of internet connection records they must explain clearly how they intend to safeguard the privacy of citizens first. They must also be 100% clear on how the technology will work.

Many technologists have expressed concern that the proposals in the draft Bill are not as straightforward as proposed. For example, concerns have been raised about how feasible it will be to separate the content of a message from an ICR.

In his evidence to the Science and Technology Select Committee **John Shaw, Vice President, Project Management at Sophos,** stated that in reality the line between content and communications data was "*incredibly blurred*".[133]

In written evidence to the same committee the **IT-Political Association of Denmark** raised further concerns about the viability of using ICRs in law enforcement investigations:

> "*Device identification seems to be the primary objective of ICRs, but there are limits as to what devices an ISP can actually identify. In general, the ISP can only identify devices that are connected directly to the ISP."*

It should be noted that Denmark had previously implemented a data retention scheme similar to the system proposed in the draft bill, these measures where repealed by the Danish Government in 2014 because "*they were unable to achieve their stated objective*" of investigating and prosecuting crime.[134]

---

[130] Clause 1, *Draft Communications Data Bill*, June 2012, p. 13: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228824/8359.pdf

[131] Guardian, *MPs call communications data bill 'honeypot for hackers and criminals'*, 31st December 2012: http://www.theguardian.com/technology/2012/oct/31/communications-data-bill-honeypot-hackers-criminals

[132] Joint Committee on the Draft Communications Data Bill, *Final Report*, 28th November 2012, p.29: http://www.publications.parliament.uk/pa/jt201213/jtselect/jtdraftcomuni/79/79.pdf

[133] J. Shaw, *Science and Technology Committee – Oral Evidence, Investigatory Powers Bill: technology issues*, p. 9 10th November 2015: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/oral/24378.pdf

[134] Ibid p. 2: http://itpol.dk/sites/itpol.dk/files/IPBill-Science-Tech-Committee-ITpol-submission-nov15-FINAL.pdf

Lack of detail in the draft Bill regarding the security of the data and how it will be held is a concern, particularly as cyber hacking and cyber security is a growing problem for all of us. In 2014 90% of large firms and 74% of small firms in the UK suffered a security breach[135]

The issue is not limited to the UK. The case of the US Office of Personnel Management breach which saw the often highly personal information of 21.5 million people hacked, as well as the recent hack of TalkTalk and indeed the hack conducted on the Ashley Madison site have shown that regardless of who is storing the information there are vulnerabilities.[136]

It is essential that detail about the requirements placed on the telecommunication services (who notably are given a broad definition in the draft Bill) are made clear. The public will want to know how their data will be protected. Will it be encrypted, where will it be held, will it be held in a cloud service, will it be held here in the UK or abroad, who will have access, how will they have access, what cyber protections will be put in place and should a hack, breach or attack occur who will be responsible?

Building and maintaining these systems to meet the Government's requirements may prove to be costly. The Government has quoted an estimate of £187.1m for this portion of the draft Bill. It is worth noting that estimates for similar earlier schemes were much higher. The Intercept Modernisation Scheme was projected to cost £2bn, whilst the draft Communications Data Bill came with an estimated price tag of £1.8bn.

In the latter case the estimates were attacked by industry experts who questioned where the figures had come from.

It is important that the Government properly identify where the costs incurred by their proposals will fall and that detail of what is defined in **Clause 185(1)** as an "appropriate contribution" is outlined.

Overall a great deal more clarity is needed over how this intrusive new power is intended to work, how proportionate the plan to retain 12 months of data really is, how effective it will be and what protections will be put in place to ensure the security of the data when retained. If the Government cannot conclusively prove that Internet Connection Records will be of operational use in the majority of cases, then they will be intruding on privacy for no discernible reason.

Communications Data

We are concerned about the definitions used to define what communications data is. The draft Bill goes to great length to provide a broad range of what is considered to be communications data and has introduced new definitions of event and entity data.

Indeed in **Sub-Clause 195(1)** we learn that "*data*" includes "*any information which is not data*." Our interpretation of this is that quite simply, anything can be defined as communications data. In a world now fueled by data this leaves little, if anything, free from potential intrusion.

Furthermore the process of authorisation for communications data is also a broad.

---

[135] HM Government, *2015 Information Security Breaches Survey*, p. 6: http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf

[136] The Atlantic, *About Those Fingerprints Stolen in the OPM Hack*, 23rd September 2015: http://www.theatlantic.com/technology/archive/2015/09/opm-hack-fingerprints/406900/

The draft Bill states throughout **Sub-Clause 46(4)** that "*any person*" can be asked for access to communications data, going so far in **Sub-Clause 46(4) (c)** as to state that "*any person whom the authorised officer believes is not in possession of the communications data but is capable of obtaining it, to obtain it and disclose it.*" This, along with **Sub-Clause 46(5) (c)** poses questions about the requirements placed on telecommunications services and their staff with regards to the data they hold and the data held by other companies.
The suggestion that the retention of "*data whether or not in existence at the time of the authorisation*" may be authorised, poses questions about necessity and proportionality and issues of pre-crime policing.
Finally we raise concern at the sheer wealth of bodies and purposes for access to communications data outlined in **Sub-Clause 46(7)**.

Bulk Powers

Of all the powers contained within the draft Bill the powers to carry out bulk interception, bulk equipment interference and the collection, retention and use of bulk personal datasets are the most intrusive for ordinary law abiding citizens. The lack of detail in the draft Bill regarding how they work in practice or how they affect members of the public is of concern, particularly as these powers have now been avowed and therefore detail of their use will be known.
We know that bulk personal datasets involve the collection and storage of the private or personal data of any and all British citizens whether dead or alive, innocent or suspect poses beyond that little detail is known, leading us to assume that any State dataset (datasets which we are all obliged without choice to appear on simply by being a British citizen) will be gathered, retained and analysed beyond the basic intended need/use of the dataset. That means birth and death records, health records and national insurance numbers to name but a few.
Should our assumption be accurate, more detail must be provided about what impact the use of these bulk personal datasets will have on the citizen including how their personal information can be intruded upon – even in the process of determining them as not being a person of interest.
The intelligence agencies have to be able to demonstrate exactly why they need these powers in bulk and what benefit bulk provides rather than the process of requesting data on a specific target in the course of an operation. To date none of this has happened.
Furthermore for the use of such data to be given the proper scrutiny and have the strongest of safeguards, the role of the Judicial Commissioner overseeing the use of the data should be strengthened.
The draft Bill proposes that the Judicial Commissioners will only have a role in reviewing the acquisition, retention use or disclosure of bulk personal datasets. It should be the case that the Commissioners are responsible for properly auditing, inspecting and investigating the use of BPDs.

It's only through proper scrutiny that the use of these powers can be justified. Of additional concern is that organisations served with a BPD warrant will not be able to query its terms.

Equipment Interference

Equipment Interference; also known as hacking or Computer Network Exploitation (CNE), has the potential to be enormously intrusive, damaging to individual devices, computer networks and systems, as well as a potential threat to the security of the internet as a whole.

The unintended consequences which can occur by the weakening of any system will enable other non-law enforcement or intelligence agency individuals to exploit the weakness, this may include malicious actors and rogue states.

In evidence to the Investigatory Powers Tribunal (IPT) **Ciaran Martin, an employee of GCHQ**, noted that Equipment interference can vary in complexity, from using the login details of a target to much more sophisticated tactics:

> "*Taking advantage of weaknesses in software. For instance a piece of software may have a "vulnerability": a shortcoming in the coding that may permit the development of an "exploit", typically a piece of software, a chunk of data, or a sequence of commands that takes advantage of the vulnerability in order to cause unintended or unanticipated behaviour to occur. This unanticipated behaviour might include allowing another piece of software – an implant called a "backdoor" or a "Trojan" – to be installed on the device.*"[137]

The lasting damage equipment interference can do to a system was highlighted by the hacking of the telecommunications firm Belgacom. The case involved three of the company's engineers being tricked into using "*spoofed*" LinkedIn and Slashdot pages which infected their machines with malware.[138] **Brian Honan, managing director of BH Consulting**, an IT consultancy firm, warned after the hack was revealed that:

> "*It would be good security practice to assume that not all instances of the malware have been identified and dealt with but rather to operate the network as if it is compromised and secure your data and communications accordingly*".[139]

Some forms of equipment interference can spread much further than originally intended. An example of this is the Stuxnet virus. Created by the United States and Israel it was originally targeted at Iran's nuclear enrichment facilities. As a result of the attack the virus "*escaped*" from the target system and infected the energy company Chevron's network. Chevron's general manger Mark Koelmel underlined the concern, noting "*I don't think the U.S. government even realised how far it had spread*".[140]

Given the clear risks involved, the proportionality of the tactic needs to be considered. Equipment interference should not be used as a bulk tactic designed to infiltrate broader systems, networks or organisations.

Big Brother Watch registered concern over collateral intrusion during the consultation on the Equipment Interference Code of Practice. The draft Bill and the re-published draft Code of Practice do nothing to alleviate the concern. It is unclear why someone who is not an "*intelligence target*" in their own right, as referenced in **Paragraph 2.12** of the **Equipment Interference Code of Practice**, would be targeted. This kind of loose wording could lead to

---

[137] C. Martin, *Witness Statement in the Investigatory Powers Tribunal between Privacy International and Secretary of State for Foreign and Commonwealth Affairs and Government Communications Headquarters*, p. 6, 16th November 2015: https://privacyinternational.org/sites/default/files/CM_Witness_Statement_Signed_2015_11_16.pdf

[138] The Intercept, *Operation Socialist; The Inside Story of How Britain's Spies Hacked Belgium's Largest Telco*, 13th December 2014: https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/

[139] SC Magazine, *GCHQ faces new Belgacom hack allegations*, 16th December 2014: http://www.scmagazineuk.com/gchq-faces-new-belgacom-hack-allegations/article/388531/

[140] Wall Street Journal, *Stuxnet Infected Chevron's IT Network*, 8th November 2014: http://blogs.wsj.com/cio/2012/11/08/stuxnet-infected-chevrons-it-network/

potential fishing trips and middle men attacks against individuals who have not been satisfactorily linked to an investigation.

The concept of fishing trips or middle men attacks are especially important when considering the role of a 'gatekeeper' to a system, such as an IT manager or system administrator. These individuals are often completely innocent and indeed unaware about the specific information the targeted individual may hold. Specific protections must be outlined to ensure collateral damage does not occur and to ensure that the intrusion on innocent people does not take place.

In its current form **Clause 81(3)** of the draft Bill risks permitting equipment interference operations to go much further than the original target of a warrant:

> "*A targeted equipment interference warrant may also authorise the person to whom it is addressed to secure—*
>
> > *(a) the obtaining of any communications, private information or equipment data to which the purpose of the warrant relates;*
> > *(b) the obtaining of any information that does not fall within paragraph (a) but is connected with the equipment to which the warrant relates;*
> > *(c) the disclosure, in such manner as may be described in the warrant, of any material obtained under the warrant by virtue of paragraph (a) or (b).*"

Sub-Clause 81(3)(b) allows for the "*obtaining of any information*" that is "*connected*" with the equipment covered by the warrant. Given the way the internet works and the myriad of ways in which information and systems can now connect with each other this could potentially enable much broader action than was intended by the original warrant.

It should be noted that there is great contradiction between the authorisation procedures for law enforcement equipment interference warrants and those granted to the intelligence services requires clarification.

Clause 89 of the draft Bill makes it clear that when law enforcement bodies apply for a warrant to use targeted equipment interference they are not required to submit an application to the Home Secretary, only to the relevant Chief Constable, followed by review by one of the Judicial Commissioners. **Clause 84** states that when the intelligence agencies seek an equipment interference warrant they are required to seek authorisation by the relevant Secretary of State followed by review by a Judicial Commissioner.

When applying to modify a warrant the two systems are again different. Under **Clause 96** law enforcement bodies must submit any changes to a Judicial Commissioner, yet this requirement is removed for the intelligence agencies. It is unclear why as the action being authorised is the same, the only thing that has changed is the requesting body. There has been no explanation for this difference in procedure.

Encryption

Encryption is a crucial part of maintaining the security of all our online engagement, from banking to health data and beyond. Having a digital presence is now no longer a choice. We are all data citizens, were that presence to be made insecure in any way we will all be placed at risk of exposure to hacking, cyber-crime, data loss or breach. In a completely connected world this will impact access and security to the basic essentials of life.

In light of this **Clause 189** of the draft Bill which would allow the Secretary of State to "*make regulations imposing specified obligations on relevant operators*". **Sub-Clause 4(c)** allows the

Secretary of State to put in place "*obligations relating to the removal of electronic protection applied by a relevant operator to any communications or data*" are a huge concern.

The importance of encryption as a tool for safeguarding the data of all citizens is recognised by a broad range of people and organisations.

For example the Information Commissioner's Office has stated that:

> "*The ICO recommends that portable and mobile devices including magnetic media, used to store and transmit personal information, the loss of which could cause damage or distress to individuals, should be protected using approved encryption software which is designed to guard against the compromise of information*."[141]

Recent headlines have shown the impact government legislation can have on the technology sector - a sector which now impacts every business whether an IT business or not and is the foundation of economic well-being of the UK.

Indeed should the draft Bill impose a requirement for companies to weaken or remove their encryption to comply with warrants, the UK could find itself a country which no technology company will want to engage with. Additionally the development of new technology companies wishing to start, grow or expand in the UK would be stifled. Several tech companies have already warned that this could be a threat to strong encryption in the UK.[142]

From a business perspective **The Information Technology Council**, a global umbrella group for technology firms has reacted strongly to any previous calls to weaken encryption:

"*Encryption is a security tool we rely on every day to stop criminals from draining our bank accounts, to shield our cars and airplanes from being taken over by malicious hacks, and to otherwise preserve our security and safety. We deeply appreciate law enforcement's and the national security community's work to protect us, but weakening encryption or creating backdoors to encrypted devices and data for use by the good guys would actually create vulnerabilities to be exploited by the bad guys, which would almost certainly cause serious physical and financial harm across our society and our economy. Weakening security with the aim of advancing security simply does not make sense.*"[143]

With regards to the impact weakening of encryption would have on ordinary people **Tim Cook, CEO of Apple** has highlighted that:

> "*If you halt or weaken encryption, the people that you hurt are not the folks that want to do bad things. It's the good people. The other people know where to go*"[144]

In the past Mr Cook has attacked calls from the US to undermine encryption stating that:

> "*We think this is incredibly dangerous. We've been offering encryption tools in our products for years, and we're going to stay on that path. We think it's a critical feature for our customers who want to keep their data secure. For years we've offered encryption services like iMessage and FaceTime because we believe the contents of your text messages and your video chats is none of our business.*"[145]

---

[141] Information Commissioner's Office, *Encryption*: https://ico.org.uk/for-organisations/encryption/

[142] Guardian, *Tech firms warn snooper's charter could end strong encryption in Britain*, 9th November 2015: http://www.theguardian.com/technology/2015/nov/09/tech-firms-snoopers-charter-end-strong-encryption-britain-ip-bill

[143] https://www.itic.org/news-events/news-releases/tech-responds-to-calls-to-weaken-encryption

[144] The Verge, *Tim Cook says UK plans to weaken encryption will 'hurt good people'*, 10th November 2015: http://www.theverge.com/2015/11/10/9703526/tim-cook-encryption-uk-investigatory-powers-bill

[145] TechCrunch, *Apple's Tim Cook Delivers Blistering Speech On Encryption, Privacy*, 2nd June 2015: http://techcrunch.com/2015/06/02/apples-tim-cook-delivers-blistering-speech-on-encryption-privacy/#.xkpdpk:kVGu

As far as the impact weakened encryption would have the country as a whole, including government agencies **Jon M. Peha, former Assistant Director of the White House's Office of Science and Technology Policy**, bluntly stated that:

> "*Individual computer users, large corporations, and government agencies all depend on the security features built into information technology products and services that they buy on the open market. If the security features of these widely available products and services are weak, everyone is in greater danger*".[146]

In an op-ed for the Washington Post **Mike McConnell, the former Director of the NSA, Michael Chertoff, former Secretary of Homeland Security and William Lynn, the former Deputy Secretary of Defence** argued that strong encryption was more important than government access to communications:

> "*We recognise the importance our officials attach to being able to decrypt a coded communication under a warrant or similar legal authority. But the issue that has not been addressed is the competing priorities that support the companies' resistance to building in a back door or duplicated key for decryption. We believe that the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server and enterprise level without building in means for government monitoring.*"[147]

Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications, is a report co-authored by the world's leading cyber-security experts, highlights the problems with the calls for scrapping or weakening encryption.

The 2015 report argues that there are three overarching problems with providing governments with "*exceptional access*".

1. Providing permanent encryption keys would diverge from the current practice of deleting keys directly after use. If a key were stolen it could compromise the entire system.
2. Allowing for this kind of access will "*substantially increase*" system complexity, with any new technology feature having to be tested by hundreds of thousands of developers around the world.
3. The security of the encryption keys is a huge problem. Creating and holding onto a key which could unlock a system would establish a weakness for if that key were to fall into the hands of an enemy it would give an attacker the ability to cause a huge amount of damage.[148]

---

[146] Jon M. Peha, *The Dangerous Policy of Weakening Security to Facilitate Surveillance*, 4th October 2013: http://users.ece.cmu.edu/~peha/Peha_on_weakened_secuirty_for_surveillance.pdf

[147] M. McConnell, M. Chertoff and W. Lynn, *Why the fear over ubiquitous data encryption is overblown*, 28th July 2015: https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html

[148] H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, M. Green, P.G. Neumann, S. Landau, R. L. Rivest, J. I. Schiller, B. Schneier, M. Specter and D.J. Weitzner, *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*, 6th July 2015, p. 2: http://www.crypto.com/papers/Keys_Under_Doormats_FINAL.pdf

The report poses 25 questions which the authors suggest "*must be answered in detail*" before any legislation to demand exceptional access is drafted.[149]
Put simply any part of the draft Bill which may have implications for the strength of encryption will have severe consequences for the people and the country as well. Any approach to weaken, create backdoors or simply abandon encryption must be treated with extreme caution.

Commissioner System

Big Brother Watch has called for reform to the Commissioner System on a number of occasions. The proposals for merging the three existing organisations into one body has the potential to solve many of the recurring issues, most notably:

1. The lack of funding in the current system.
2. The poor staffing of the current commissioners' offices.
3. The limited scrutiny the commissioners can provide.

The success or failure of the new scheme will rest largely with what kind of resources the Investigatory Powers Commission (IPC) is given to do its job.
Sub-Clause 176(1) notes that the Treasury will have the final say on what level of resourcing the IPC will have. This is sensible, but it is important that the process of arriving at the final figure is conducted in an open way with a broad consultation. This makes **Sub-Clause 176(2)** troubling. It stipulates that the Secretary of State must arrive at a decision on this matter based on consultation with only the Investigatory Powers Commissioner.
It would be preferable for the legislation to require consultation with a much broader range of individuals and organisations including those outside of government. The IPC will be an important part of whatever system is decided upon and this means it is vital its funding and staffing structure is properly debated. Only through this approach will citizens be assured that the intrusive powers contained within this draft Bill are overseen effectively and that the proposed system will really be an improvement.
Sub-Clause 167(1) giving the Prime Minister the power to appoint the Chief Judicial Commissioner and the Judicial Commissioners concentrates too much power in the hands of the Executive and will prevent any real independence of the Commission.
An alternative would be to allow the Judicial Appointments Commission (JAC) to make the decision on who is appointed to each position. The JAC already has a role in appointing circuit court judges, High Court judges and UK judges on the European Court of Human Rights (ECtHR). This system would give the IPC a better chance of being a properly independent body.

Interception

Sub-Clause 26(2), the modification of warrants; allows for names to be added or removed, descriptions of people to change, organisations or premises to be changed, indeed any factor specified on the original warrant can be internally changed with no further review by a Judicial Commissioner.
It is important that every modification receives a high level of scrutiny; preferably with an independent Judicial Commissioner authorising not reviewing any changes. This will provide a safeguard for the citizen.

[149] Ibid, p. 21: http://www.crypto.com/papers/Keys_Under_Doormats_FINAL.pdf

The **draft Code of Practice for interception**, published alongside the draft Bill also raises concern about the protection of the citizen. In **Paragraph 4.1** it states that

> "*Should an interception operation reach the point where individuals other than the subject of the authorisation are identified as investigative targets in their own right consideration should be given to applying for separate warrants covering those individuals."*[150]

It should be a requirement to apply for a new interception warrant when targeting an individual who isn't the subject of the original warrant. When a new individual, previously not named by the warrant, can be proven to be of interest, it should be the case that a new warrant is sought before that individual's communications are intercepted.

Clause 42 maintains the bar on using intercepted material in court. Currently the UK is the only country that operates a common law system which entirely outlaws the use of intercept evidence in court.

Removing the bar is supported by a number of organisations and individuals including Big Brother Watch. **David Anderson QC, the Independent Reviewer of Terrorism Legislation** has stated that "*all right-minded people would like to see intercept evidence admissible in our courts*".[151]

Stuart Osborne, former Senior National Coordinator of Counter Terrorism and Head of the Counter Terrorism Command also commented that as part of a "*wide package of measures*" intercept evidence "*could be very useful in prosecution cases*."[152]

Countries which allow the use of intercept evidence include the US, Australia and New Zealand.

Asked about the effectiveness of this **technique former Australian Commonwealth Director of Public Prosecutions, Damian Bugg QC** said: "*The use of telephone intercepts in trials for terrorism offences and other serious crimes is now quite common in Australia and I cannot understand why England has not taken the step as well.*"[153]

The effectiveness of introducing intercept evidence can be clearly seen in America. **JUSTICE** conducted a review of 10 US terror plots which involved a total of 50 individuals. With the help of intercept evidence the authorities secured both charge and conviction in each case and all within the 48 hour pre-charge detention limit. Concluding, the report argued that "*the key difference between UK and US terrorism investigation appears to [be] the extensive reliance by the police and FBI on intercept evidence in prosecuting suspected terrorists.*"[154]

The continued refusal of the Government to consider allowing intercept evidence to be used in court is made more confusing by the fact that evidence gained through equipment interference is permitted. The argument that the evidence from intercepting communications would reveal too much about the methods and work of the intelligence

---

[150] Home Office, *draft Interception Code of Practice*, 4th November 2015, p. 10: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473845/6.1276_151104_INTERCEPTION_CoP_for_designer_FINAL_WEB.PDF

[151] Joint Committee on the Draft Enhanced Terrorism Prevention and Investigation Measures Bill, *Report*, 27th November 2012, p. 28: http://www.publications.parliament.uk/pa/jt201213/jtselect/jtdraftterror/70/70.pdf

[152] Ibid p. 29

[153] D. Raab, *Fight Terror, Defend Freedom*, September 2010, p. 39: http://www.bigbrotherwatch.org.uk/files/dominicraabbookfinal.pdf

[154] 6 JUSTICE, *From Arrest to Charge in 48 Hour: L Complex terrorism cases in the US since 9/11*, November 2007: http://www.justice.org.uk/data/files/resources/37/From-Arrest-to-Charge-in-48-Hours-1-November-2007.pdf

agencies seems nonsensical when it is permitted in a power which only recently has been avowed. Further information on why it is not possible to utilise this evidence in court would be instructive.

The draft Code of Practice for interception adds more questions. **Paragraphs 8.6 to 8.10** of the Code allow intercepted material to be disclosed to a prosecutor to help him or her "*determine what is required of him or her by his or her* duty to *secure the fairness of the proceedings*".[155] There is little information about how a disclosure of this kind would help increase the fairness of a trial. Similar passages allow for the release of information to a judge.

This is especially prescient given the fact that **Paragraph 8.14** concludes that "*nothing in these provisions allows the intercepted material, or the fact of the interception, to be disclosed to the defence*."[156] The document should at the very least outline the circumstances which could lead to a disclosure and the reasons why materials can be released to a judge and a prosecutor but not those acting for the defence.

Redress/User Notification

The draft Bill barely touches the issue of redress. **Clause 180**, which would allow an appeal to be brought in a UK court as opposed to the European Court of Human Rights (ECtHR), is a small step in the right direction. However questions about how it will work in practice need to be answered.

Sub-Clause 180(1) notes that appeals may be brought on a "*point of law*". This implies that appeals may only be brought on the Tribunal's interpretation of legal principles. Clarity must be provided on whether or not appeals can be made for errors of fact or procedural unfairness as well. If this is not the case an explaniation should be provided as to why the Government rationale for limiting the grounds for appeal.

Sub Clause 180(4) also raises issues:

> "*The Tribunal or court must not grant leave to appeal unless it considers that—*
>
> *(a) the appeal would raise an important point of principle or practice, or*
>
> *(b) there is another compelling reason for granting leave.*"

It is unclear whether this could be used to further limit the instances under which someone could appeal a decision by the Investigatory Powers Tribunal (IPT).

Sub clause 171(1) makes clear that the IPT must inform a person of any error relating to that person, however **Sub-clause 171(2)** requires clarification. It states that before any report is made, both the IPT and the IPC must agree that an error has taken place and that disclosure would be in the public interest. More information is needed about how decisions will be arrived at and in particular how the public interest test will be applied.

A proper system of redress is vital to ensuring that the citizens can be confident that these powers are being used in their best interests. The draft Bill currently fails to do that.

Big Brother Watch have called for reform in this area for a number of years. Any workable system must begin with some form of user notification. Germany, Belgium and from 2016 the State of California will all use a system of user notification so it isn't a new or indeed unique proposal.

---

[155] Home Office, *Draft Code of Practice for the Interception of Communications*, 4th November 2015, p. 32: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/401866/Draft_Interception_of_Communications_Code_of_Practice.pdf

[156] Ibid, p. 33

Innocent individuals are informed that they have been the target of surveillance once the case has been closed.
If the same process were adopted in the UK it would increase the amount of transparency as well as provide an opportunity for redress - allowing the individual to clear their name. Previously we have stated that notification should take place 12 months after the conclusion of an investigation. Under the proposals there would also be the opportunity to apply to a judge to extend this period in 6 monthly increments.[157]
Fundamental change to the way the Investigatory Powers Tribunal functions is necessary and is lacking from the draft Bill.

The Royal United Services Institute's (RUSI) *Democratic Licence to Operate* contains a number of recommendations which would help the IPT "*make its business less opaque to the public*".[158]At present the IPT is far too secretive. At the very least it should adopt RUSI's recommendation of holding open hearings.[159] This would help increase public confidence in its work and in the process increase awareness of the work the Tribunal does. It should be noted that this would not preclude the Tribunal from holding secret proceedings when it could be demonstrated that there was a pressing need to do so.

Terminology

Finally, it should be noted that throughout the draft Bill terms are often very loose or broadly described. For surveillance legislation to be meaningful and for the general public to be reassured and have a comprehensive understanding of what terms mean, how techniques and powers can be used and who will have access to or hold their data, the Bill should look to offer further clarity. This is not to divulge the secrets of the operation but to be precise rather than vague.

8 December 2015

[157] Big Brother Watch, *Off the Record: How the police use surveillance powers*, October 2014, p. 8: http://www.bigbrotherwatch.org.uk/wp-content/uploads/2014/10/Off-the-Record-BBW-Report1.pdf
[158] Royal United Services Institute*, A Democratic Licence to Operate*, 13th July 2015, p. 113: https://rusi.org/sites/default/files/20150714_whr_2-15_a_democratic_licence_to_operate.pdf
[159] Ibid p. 113

Paul Biggs—written evidence (IPB0084)

Privacy is a fundamental human right. I am against the Government treating all UK citizens as suspects via surveillance and invading our online and telecommunications privacy:

1. No surveillance without suspicion

Mass surveillance must end. Surveillance is only legitimate when it is targeted, authorised by a warrant, and is necessary and proportionate. A new warrantry system that increases the threshold for authorising surveillance is required.

2. Transparent laws, not secret laws

The Government is using secret agreements and abusing archaic laws. We need a clear legal framework governing surveillance to protect our rights. The public should be informed of the powers that are available to the intelligence agencies to interfere with the right to privacy, as well as the process for the authorisation of such a power.

3. Judicial not political authorisation

Ministers should not have the power to authorise surveillance. All surveillance should be sanctioned by an independent judge on a case-by-case basis. There needs to be a clear international framework for the accessing and sharing of data between companies and governments. This could be delivered through improvements to the Mutual Legal Assistance Treaty (MLAT) as advised in Sir Nigel Sheinwald's recent report to the Prime Minister, which should be made public.

4. Effective democratic oversight

Parliament has failed to hold the intelligence agencies to account. Parliamentary oversight must be independent of the Executive, properly resourced, and able to command public confidence through regular reporting and public sessions. DSOU supports calls for a new independent body to be staffed with technical, legal and investigative experts who have relevant expertise, including in privacy and civil liberties. The Intelligence and Security Committee (ISC) should report to Parliament not the Executive and be chaired by a Member of the Opposition. It should be empowered to make decisions on reporting and publications and be appropriately funded and staffed.

5. The right to redress

Innocent people have had their rights violated. Everyone should have the right to challenge surveillance in an open court. The Right of appeal should be part of any new surveillance law. The Investigatory Powers Tribunal (IPT) should hold open hearings and there should be the right to appeal the IPT's decisions. Individuals who are subject to surveillance should be legally notified when there is no risk to jeopardising an ongoing investigation. This should ordinarily happen within12 months of the conclusion of the investigation, although that 12-month period may be extended in six-month intervals by judicial authorisation. Consideration must be given to how citizens are able to seek redress if they have no means to find out if they have been subjected to surveillance.

6. A secure internet for all

Weakening the general security and privacy of communications systems erodes protections for everyone, and undermines trust in digital services. The Government should cease breaking encryption standards and undermining internet security; such activity should be explicitly prohibited by legislation.

21 December 2015

Bingham Centre for the Rule of Law—written evidence (IPB0055)

SUMMARY

The Bingham Centre for the Rule of Law welcomes the government's attempt to put certain investigatory powers on a clearer statutory footing and to increase the safeguards, accountability and transparency associated with the exercise of such powers. We also welcome the oversight changes that will see the establishment of a single commission and new rights of appeal from decisions of the Investigatory Powers Tribunal. The Bingham Centre's view is that the Draft Bill could be substantially improved to enhance fidelity to the rule of law and public confidence, while still ensuring that law enforcement, the intelligence agencies and Secretaries of State have appropriate and adequate powers to combat national security threats and serious crime. Our recommendations are made to that end. The submission has three parts.

PART 1: THE BINGHAM CENTRE AND ITS PRIOR WORK ON INVESTIGATORY POWERS [paras 1-6]

The Centre is a leading rule of law organisation. Its prior work on investigatory powers included a detailed submission to the review by David Anderson QC. In *A Question of Trust*, Mr Anderson referred to the Centre's submission on a number of occasions and, perhaps most significantly, took up the Bingham Centre's position in making his recommendation for judicial authorisation of warrants and the use of a Judicial Commissioner model (see para 14.47, *A Question of Trust*).

PART 2: THE RULE OF LAW, ANALYSIS OF DRAFT BILL, RECOMMENDATIONS [paras 7-55]

We outline what the rule of law is and how it is applies in the context of the Draft Bill. We analyse the Bill, focusing mainly on oversights, warrants and authorisations, and make 12 recommendations:

1: Judicial authorisation is to be preferred to the proposed 'double-lock' (Parts 2, 3, 5, 6, 7). However, our remaining recommendations apply whether judicial authorisation is used or the 'double-lock' is retained.

2: Serious crime warrants should be on application by law enforcement and issued by judges.

3: Applications for warrants (eg, Cl 14(6), 84(6), 107(5), 122(4), 137(4), 153(2), 154(4)) and criteria for authorisations (eg, cl 46) and the giving of notices (eg, cl 72, 188) should be required to identify other, less instrusive options that have been considered and rejected.

4: In urgent circumstances, subsequent approval should be within 48 hours, not 5 days (cl 20, 91, 156, see also cl 119, 147, 160).

5: Journalistic sources (clause 61) – warrants should be made subject to additional safeguards.

6-7: Special advocates should be used where sensitive confidential communications are in issue and where novel or contentious applications are made.

8: National security notices (clause 188) – these should be subject to additional safeguards.

9: Judicial commissioners (clause 168) – appointments should be for non-renewable terms and 'inability or misbehaviour' removals should require parliamentary approval

10: Notification of serious errors (clause 171) – presumption should be that there is notification and, in exceptional circumstances, notifcation shoud not be denied but should be deferred and reviewed every 5 years.

11: Annual reporting (clause 174) – sensitive communications should be included in statistical requirements.

12: Codes of Practice - Legal Professional Privilege (clause 179 / Sched 6)– should be in the body of the Act rather than a code of practice.

PART 3: CONSOLIDATED LIST OF RECOMMENDATIONS [pages 13-16]

For convenience, we provide a consolidated list of recommendations.

PART 1: THE BINGHAM CENTRE AND ITS PRIOR WORK ON INVESTIGATORY POWERS

Introduction

1. The Bingham Centre for the Rule of Law welcomes this opportunity to submit evidence to the Joint Committee on the Draft Investigatory Powers Bill.

2. The Bingham Centre for the Rule of Law was launched in December 2010 to honour the work and career of Lord Bingham of Cornhill – a great judge and passionate advocate of the rule of law. The Centre is dedicated to the study, promotion and enhancement of the rule of law worldwide. It does this by defining the rule of law as a universal and practical concept, highlighting threats to the rule of law, conducting high-quality research and training, and providing rule of law capacity-building to enhance economic development, political stability and human dignity. The Centre is a constituent part of the British Institute of International and Comparative Law (BIICL), a registered charity and leading independent research organisation founded over 50 years ago.

3. The Centre has engaged with investigatory powers issues for some time. Of particular note, in November 2014 **the Centre made a detailed submission to the review by David Anderson QC** (available at http://www.biicl.org/documents/399_bingham_centre_submission_to_investigatory_powers_review_final__2014-11-19.pdf). In *A Question of Trust*, Mr Anderson referred to the Centre's submission on a number of occasions and, perhaps most significantly, **Mr Anderson took up the Bingham Centre's position in making his recommendation for judicial authorisation of warrants and the use of a Judicial Commissioner model** (see para 14.47, *A Question of Trust*).

4. In this submission we avoid revisiting the detailed analysis contained in our November 2014 submission. Conscious of the volume of submissions the Committee will receive

and in light of the breadth of the Draft Bill, we address only a limited range of issues in relation to which we have most expertise, attempt to present rationales concisely and make some specific recommendations. We would of course be happy to provide further written or oral evidence should it assist the Committee.

5. This submission has been written by Dr Lawrence McNamara (Acting Director & Senior Research Fellow, Bingham Centre for the Rule of Law) and Dr Eric Metcalfe (Barrister, Monckton Chambers, and Fellow of the Bingham Centre).

6. This submissin is framed around the call for evidence by the **Joint Committee on the Draft Investigatory Powers Bill** and submitted to that Committee as written evidence. Following that, it has been sent on the same day to the **Joint Committee on Human Rights** as a response to the JCHR's call for evidence on the Draft Bill.

PART 2: THE RULE OF LAW, ANALYSIS OF DRAFT BILL, RECOMMENDATIONS

The Draft Bill on the whole

7. The Bingham Centre welcomes the government's attempt to put certain investigatory powers on a clearer statutory footing and to increase the safeguards, accountability and transparency associated with the exercise of such powers. It represents a substantial step forward in these respects. We also welcome the oversight changes that will see the establishment of a single commission and new rights of appeal from decisions of the Investigatory Powers Tribunal.

8. The Centre's view is that nevertheless the Draft Bill could be substantially improved to enhance fidelity to the rule of law and public confidence, while still ensuring that law enforcement, the intelligence agencies and Secretaries of State have appropriate and adequate powers to combat national security threats and serious crime. Our recommendations are made to that end.

A. Overarching / thematic questions: necessity and legality

Investigatory powers: challenges and fidelity to the rule of law

9. It is beyond question that the state has a particular responsibility to protect the public from serious crime, including acts of terrorism. It is essential that law enforcement and intelligence agencies have investigatory powers that enable the government to fulfil that responsibility. Such powers may require intrusive acts (including surveillance, data access and equipment interference) and they may require secrecy and the curtailment of rights to a fair hearing and effective remedy. It is equally beyond question that these powers cannot be unlimited; the extent and exercise of such powers are subject to the rule of law.

10. As Tom Bingham has observed in his landmark work, *The Rule of Law*, the rule of law is not a vague concept but contains concrete principles that can be identified and applied as standards against which laws can be made. The founding Director of the Bingham

Centre, Professor Sir Jeffrey Jowell QC, has developed these arguments (eg, J Jowell, 'The Rule of Law: A Practical and Universal Concept' 2014). Several components of the rule of law are particularly relevant in our analysis of the Draft Bill. Among them:

- The rule of law requires that laws are clear and certain.
- The rule of law requires access to justice, and this demands that there are fair hearings, with equality of arms, before independent judiciaries.
- The rule of law requires legality. This demands not only that the powers of the executive are exercised under law, but also that executive powers are not overly broad. Excessive discretion is at most a temptation to arbitrariness and at least can lead to a neglect or undermining of interests in privacy and access to information.

The rule of law is the cornerstone of democratic accountability and public trust in the state. Fidelity to the rule of law enhances public trust in the state, such that over the longer term it enables the government to effectively discharge its key responsibility of protecting the public.

11. In practical terms, the rule of law requires that there are meaningful and appropriate limits on the scope of investigatory powers, and there are meaningful and appropriate safeguards in place for the exercise of powers that parliament grants to the executive. The langauge and standards of necessity and proportionality should be the watchwords throughout.

12. The government's commitment to rule of law principles does not seem in doubt. For example, as the government observes in its impact assessments, 'It is essential for public confidence that there is no doubt over the role played by those authorising action, and safeguards are seen to be explicit and stringent.'

13. The challenge is to ensure that the legislation is compatible with rule of law principles. In the recommendations that follow we identify points at which the legislation, in our view, does not adequately and appropriately meet rule of law standards, and suggest ways in which it could be changed to do so, whilst in no way diluting the capabilities of the executive to discharge its protective responsibilities.

B. Overarching / thematic questions: are the powers sufficiently supervised? Specific questions, including general, urgency and oversight

14. **Power to issue warrants/authorisations – Parts 2, 3, 5, 6, 7 – judicial authorisation rather than 'double lock' procedures:** While the 'double-lock' on the most intrusive warrants is an improvement on the previous position, we are concerned that this may not be the most appropriate method. It does not provide a suitable safeguard on the exercise of power by the Secretary of State because the balance of power to authorise weighs too heavily in favour of the executive. As well as being a Judicial Commissioner model where appointment is executive-driven (rather than authorisation by a judge *per se* who has judicial independence in the accepted sense), the standard of review is that of judicial review, and the judge must authorise in the absence of finding irrationality (in the Wednesbury unreasonable sense), albeit with the caveat that necessity and proportionality will be considered in the equation the more that an authorisation would result in an infringement of rights. Moreover, it is not necessary that the executive hold

this degree of power. Authorisation should be by Judicial Commissioners, on the application of the Secretary of State.

15. A key point of contention has been just how substantial the powers and review will be in effect. As Lord Pannick QC noted in an early comment on the Draft Bill (The Times, 12 November 2015), and as we note above, judicial review principles may encompass more than just Wednesbury-unreasonableness. However, as Lord Pannick observes in his piece, there is an important and inherent margin of discretion accorded to the executive in national security matters and judges will be sensitive to the expertise and responsibility of ministers. Lord Pannick points to difference between the Draft Bill and the position in (for example) TPIMS and control orders, with the position in the Draft Bill being that the judicial commissioner will not hear representations by the adversely affected party. That difference is profoundly important and has significant implications: the fact that the judicial commissioners will not have the benefit of *inter partes* argument as to the appropriate intensity of review will, in our view, make it highly unlikely that a judicial commissioner will stray beyond conventional Wednesbury principles. In the absence of adversarial challenge or, at least, a special advocate to present the case for those affected by the warrant, it is the commissioner who will need to both identify the arguments that might be put by those affected (were they represented) and also then judge the arguments himself or herself. In their current form, we consider that the proposals in the Bill do not adequately provide standards of access to justice or fairness that the rule of law requires.

16. We note and appreciate the ISC concern that democratic accountability rests with the Secretary of State, but a Judicial Commissioner authorisation still provides for this by virtue of the very fact that the the Secretary of State is *applying* for the warrant.

17. We appreciate also the concern that the Secretary of State has a wider picture of the relevance of any given exercise of power. However, this can be put to a Judicial Commissioner. As is well-established, judges defer greatly to the executive in security matters and a Judicial Commissioner would not refuse a warrant when confronted with a reasonable case put forward by the Secretary of State. The judicial authorisation model recommended by David Anderson QC in *A Question of Trust* provides a protection against the possible excessive exercise of power in two respects. First, it provides an independent assurance authorisation is in any given application is necessary and proportionate. Secondly, putting an application to an independent judicial commissioner will have a systemic effect, ensuring not merely scrutiny but also the independent demands that maintain over time the thresholds for authorsation, helping ensure that thresholds are not relaxed over time.

18. We differ from Mr Anderson with respect to his view that there were some categories of warrants which should have what is now the ‘double-lock’ approach, these being national security cases relating to foreign policy or defence and bulk warrants. In our view the rationale and practicality for judicial authorisation should apply to these categories as to others.

19. Public confidence in the state and its agencies will be improved by a judicial authorisation process where the judge decides an application on its merits and not merely reviews the reasonableness or rationality of the secretary of state's decision. The necessary and proportionate exercise of investigatory powers will not be diminished by a judicial process, and it will provide a check on the exercise by the executive of broad, discretionary power.

20. Recommendation 1: Where the 'double-lock' system proposed in the Bill (Parts 2, 3, 5, 6, 7), there should instead be a process in which there is:
    - An application by the Secretary of State to a Judicial Commissioner.
    - Authorisation should be by Judicial Commissioner, with the test being necessity and proportionality.

    In the event that that the 'double lock' is retained, the standard for judicial approval should expressly be necessity and proportionality.

21. It should be noted that all of the following recommendations all still apply even if the 'double-lock' is retained. That is, recommendations 2-12 are not dependent on a shift to judicial authorisation.

22. **Power to issue warrants – serious crime:** As the *Factsheet – Authorisation* indicates, 68% of the 2,795 interception warrants issued in 2014 related to serious crime. The same factsheet notes that both the RUSI report and the Anderson report recommended Judicial Commissioner authorisation for warrants in relation to serious crime. We are very strongly of the view that the RUSI and Anderson views should be followed here. In particular, there would be a substantial benefit in that the Secretary of State's attention could be more focussed on applications related to other matters, especially where national security matters are in issue and the Secretary of State's views will be of particular importance and informed by wider strategic perspectives and intelligence.

23. Recommendation 2: Serious crime warrants should be on application from law enforcement and made by judicial authorisation.

24. **Power to issue warrants, authorisations and notices – content of an application:** The supervision of warrants, authorisations and notices would be enhanced if the Secretary of State, judicial commissioner or other relevant person considering the application was provided with detail which included an outline of the options for obtaining the relevant data and confirmation that other less intrusive options have been tried but failed or have not been tried because they were bound to fail. The Draft Bill is inadequate and inconsistent and not adequate in its approach to these concerns. As it standst:
    - some provisions require consideration of whether information could reasonably have been obtained by other means (eg – those for warrants at cl 14(6), 84(6), 107(5), 122(4), 137(4))
    - some are silent on consideration of alternatives (eg – those for authorisations at cl 46 and those for notices at cl 72, 188)

- some specify what applications must obtain (eg, those for warrants at cl 153(2), 154(4)), though do not require applications to address less intrusive otpions and are silent on consideration of alterantives

Where intrusive powers are to be exercised it is appropriate that there is consideration of whether there are other, less intrusive alternatives. While this will presumably be a part of the consideration of whether information could have been reasonably been obtained by other means, it seems essential that the decision-maker be provided with the information that will enable an informed judgment, and that this is expressly required by the law.

25. Accordingly, the legislation should include, for each of the powers, a requirement that an application for a warrant outline of the options for obtaining the relevant data and confirmation that other less intrusive options have been tried but failed or have not been tried because they were bound to fail. For authorisations or notices not made on application, the same criteria should apply. An example of such a measure is found in PACE Schedule 1(2). That example relates to journalistic material, but in the Draft Bill where the scope of powers is so wide – not least in bulk collection – it would be appropriate to ensure that the material provided in an application so that it is possible to make a more informed judgment about whether the proposed measures are necessary and proportionate.

26. Recommendation 3: Applications for warrants (eg, Cl 14(6), 84(6), 107(5), 122(4), 137(4), 153(2), 154(4)) should be required to include:
    - an outline of the options for obtaining the relevant data and
    - confirmation that other less intrusive options have been tried but failed or have not been tried because they were bound to fail

    The same considerations should be required for authorisations (eg, cl 46) and notices (eg, cl 72, 188). In addition, the criteria for warrants, authorisations and notices should always include consideration of whether the information could be reasonably obtained by other means.

27. **Power to issue warrants – urgent circumstances:** Executive authorisation in urgent circumstances is appropriate and the Draft Bill rightly provides for that. However, judges are well acquainted with being available day and night for urgent matters, and one could reasonable expect that a duty roster for Judicial Commissioners would be a fairly standard expectation. Accordingly, the 'fifth working day' provision seems unnecessarily long period before authorisation could be made or approved. A more appropriate period would be 48 hours. If necessary, it could be that the statute should provide that, at the least, a provisional authorisation within 48 hours that is to be confirmed within a further 72 hours.

28. Recommendation 4: Where an executive warrant or authorisation has been issued in urgent circumstances, judicial authorisation (or approval) should be within 48 hours, rather than five working days (cf. clauses 20, 91, 156, see also cl 119, 147, 160).

29. **Power to issue warrants/authorisations – clause 61 – journalistic sources:** We welcome the inclusion in the Draft Bill of a clause recognising the public interest in the protection of journalistic sources and providing some safeguards in this area. It is right in our view that there should be no blanket exception to the powers relating to journalistic sources (though we are not sure that a blanket exception has been proposed by any stakeholders). Nevertheless, in light of the central role of journalism in maintaining a democratic society, and the importance of the protection of journalistic sources, as set out in *Mersey Care NHS Trust v. Robin Ackroyd* [2003] EWCA Civ 663 at [70]; *Financial Times v United Kingdom* (821/03) judgment 15 December 2010,[160] at [59-70] and *Goodwin v United Kingdom* (17488/90) judgment 27 March 1996,[161] at [39]ff,[162] we are of the view that the safeguards should be stronger where an application for an authorisation relates to the identification or confirmation of journalistic sources. The need for strong protections is especially important given given the breadth of purposes and interests covered in cl 46(7).

30. First, regarding clause 61(1)(a), it is not clear that there is a case for providing an exception for intelligence services from the safeguards. In the absence of a clear stated and compelling case, the better position is that the safeguards should apply to all applications, including those from the intelligence services.

31. Secondly, clause 61(1)(a) limits the safeguard to circumstances where an authorisation is sought 'for the purpose' of identifying or confirming a source. This is too narrow. It does not take into account the fact that collateral or incidental disclosures of journalistic sources cause the same damage to press freedom and therefore raise the same public interest concerns. Accordingly, our view is that the safeguard needs to apply whenever authorisation is likely to result in the identification or confirmation of a source.

32. Thirdly, clause 61(4) is in our view inadequate in two important respects. First, 61(4) suggests that notification could be provided but does not have to be. Instead, conditions should be laid down providing for when notification is not required. As to 61(4)(b), it seems to us that in this key area, there should be a presumption in favour of notifying legal representatives, particularly as journalists are commonly working within large media organisations with in-house counsel. The lawyers in these organisations are officers of the court and fully understand their duties and obligations. They are thoroughly familiar with undertakings of confidentiality (eg, the numerous 'super-

[160] http://hudoc.echr.coe.int/eng?i=001-96157
[161] http://hudoc.echr.coe.int/eng?i=001-57974
[162] Ibid: [39]. 'Protection of journalistic sources is one of the basic conditions for press freedom, as is reflected in the laws and the professional codes of conduct in a number of Contracting States and is affirmed in several international instruments on journalistic freedoms (see, amongst others, the Resolution on Journalistic Freedoms and Human Rights, adopted at the 4th European Ministerial Conference on Mass Media Policy (Prague, 7-8 December 1994) and Resolution on the Confidentiality of Journalists' Sources by the European Parliament, 18 January 1994, Official Journal of the European Communities No. C 44/34). Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public-watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected. Having regard to the importance of the protection of journalistic sources for press freedom in a democratic society and the potentially chilling effect an order of source disclosure has on the exercise of that freedom, such a measure cannot be compatible with Article 10 (art. 10) of the Convention unless it is justified by an overriding requirement in the public interest.'

injunction' cases), including in security-related cases (eg, the *Incedal* case). Where a lawyer can be identified, it seems to us neither necessary nor appropriate for the intention to seek authorisation for identification or confirmation of the source not be notified to the lawyer, so as to enable submissions to be made to the judicial commissioner on the relevant issues.

33. Accordingly, the position in clause 61(4) needs to be reversed with respect to (2)(b) to meet the requirements of the case law as set out above and more generally. That is, notice should be given unless there are good reasons not to notify the person and their legal representatives, and criteria should be set down for such determinations.

34. Fourthly, clause 61(7) provides a very narrow definition of the 'source of journalistic information', one that is unnecessarily limited by reference to the knowledge and intent of the person *supplying* the information rather than the person *receiving* it. The need for a broad definition is especially important given that the European Court of Human Rights has repeatedly held that the protection of Article 10 ECHR applies not just to professional journalists but to all those engaged in the gathering of information in the public interest, including non-governmental organisations: see e.g. *Társaság a Szabadságjogokért v Hungary* (37374/05, 14 April 2009) at para 27; *Steel and Morris v United Kingdom* (68416/01, 15 February 2005) at para 89. We recommend, therefore, that the definition of "source" in clause 61(7) be "any person who provides information to a journalist" and "journalist" as "any natural or legal person who is engaged in the collection and dissemination of information to the public via any means of mass communication".[163]

35. Fifthly, we note that clause 61 applies only to the protection of journalistic sources but provides no protection in respect of requests to access communications data that may be used to identify various other categories of confidential information, e.g. a person's medical history, or their confidential communications with ministers of religion, Members of Parliament or lawyers. Given the obvious sensitivity of communications data, we consider that it is essential that similar protection should be afforded to these categories of confidential information as well.

36. <u>Recommendation 5:</u> Amendments should be made to clause 61:

    (a) Cl 61(1)(a): there should be no exception for intelligence services.

    (b) Cl 61(1)(a): the safeguards should not apply only when the authorisation is sought 'for the purpose' of identifying or confirming a source, but should apply when it is 'likely' that an authorisation will result in disclosure of a source.

    (c) Cl 61(4)(b): this should be reversed so that where there are pre-existing legal representatives for the person to whom the authorisation relates then those representatives must be notified unless there are reasons for not notifying, and criteria for deciding on notification should be set out. Where there is not

[163] These definitions are based on (but not identical to) those set out in Recommendation No. R(2000) 7 on the right of journalists not to disclose their sources of information, adopted by the Committee of Ministers of the Council of Europe on 8 March 2000.

notification, we recommend the use of Public Interest Special Advocates (see below and Recommendation 6).

(d) Cl 61(7): The definition should be widened so that "source" in clause 61(7) is "any person who provides information to a journalist" and "journalist" is "any natural or legal person who is engaged in the collection and dissemination of information to the public via any means of mass communication".

(e) We also draw attention to recommendation (3) above, which proposes that a part of the PACE model apply generally to the Draft Bill. At the very least, the recommendation (2) provisions should apply to clause 61.

(f) We raise the question of whether protection of the confidentiality of journalistic sources in respect of requests for communications data should also be extended to other established categories of confidential information, i.e. legal professional privilege and communications with Members of Parliament, with doctor-patient confidentiality and communications with ministers of religion also arguably warranting enhanced safeguards.

37. **Power to issue warrants/authorisations – sensitive confidential communications – inter partes consideration and special advocates.** The Committee has rightly paid attention in oral evidence sessions to sensitive confidential communications, including those relating to journalistic sources and legal professional privilege, and recent parliamentary debates paid substantial attention to the position of MPs. We welcome the Committee's concerns and, in our view, there are needs for particular safeguards in these areas because they each relates to well-recognised public interests.

38. The Draft Bill proposes that applications for warrants and authorisations will be made in the absence of representations from the affected parties. However, there is no reason why this needs to be the case, and many compelling reasons why it should not be the case in all circumstances. In our view, the Committee should look closely at ways of restoring equality of arms in the authorisation process. This is especially important where there are signfiicant public interests at stake, such as those that arise in relation to sensitive confidential communications in well-established categories.

39. We note the suggestion of Lord Pannick QC that the bill 'might make provision for counsel to the judiciary, or special advocactes to ensure relevant points are addressed' (The Times, 12 November 2015). One problem that could arise, however, is the practicality of using special advocates in all circumstances, especially given the number of warrants and authorisations that may be sought, and so we give special consideration here to those established public interests (recommendation 6) and to novel or contentious applications (recommendation 7). We are also cautious in advocating what follows, as it risks a tendency to normalise secrecy and the inequality of arms in proceedings. However, on balance, we feel that with an alternative of no representation at all, a special advocate structure is preferable.

40. Recommendation 6: We would propose that where a warrant, if issued, would authorise access to sensitive confidential communications (including at least those relating to journalistic sources, MPs communications, and legal professional privilege) then the Judicial Commissioner should be required to make a two-stage decision:

    (i) To consider whether an inter partes hearing is viable, including whether it may be viable to notify identifiable legal representatives of a person affected (with undertakings of confidentiality by those lawyers). If an inter partes hearing is viable then the application should proceed on that basis. If a special advocate need to be appointed for part of the hearing then that should occur.

    (ii) If an interpartes hearing is not viable then the second stage is proceeded to: then a special advocate should be appointed so that a juducial authorisation is not made in the absence of submissions that would be made if the hearing were inter partes. In recognition of the public interest that underpins the well-established and long-accepted rationales for protections associated with these categories of sensitive communications, and of the importance of hearing submissions on both sides in arriving at a fully informed decision on such important matters, the use of special advocates in these circumstances is appropriate.

41. **Power to issue warrants – novel or especially contentious applications – Special Advocates and open judgments:** As David Anderson QC observed in *A Question of Trust*, applications for novel or contentious authorisations or warrants need to be treated with particular care (Anderson recommendations 70-71). Similarly, the resolution of novel or contentious questions needs to be conveyed to the public, especially where legal issues and interpretations of the law arise.

42. Recommendation 7: Where an application for a warrant or authorisation is novel or raises especially contentious issues (including the possible interpretation of a statute that would see an expansion of powers that differs from what is apparent on the face of the legislation) then:

    (a) a special advocate should be appointed, and
    (b) a decision on the legal issues should be published.

43. **National security notices**: Clause 188 creates a power to issue national security notices. This is an exceptionally broad power that captures matters not expressly foreseen in Parts 1-7. To some extent, the same may be said of the technical capacity notices. However, the national security notices are particularly troubling because, being in effect a residual catch all, there is inherent uncertainty as to just what the scope and exercise of the power might capture. As events have shown, uncertainty should give rise to great concern. For example, it has only recently emerged that the existing power to issue notices under section 94 of the Telecommunications Act 1984 was used by the intelligence services to obtain communications data in bulk from telecommunications providers, and this is now the basis for the bulk acquisition warrants under chapter 2 of

Part 6 of the Draft Bill. While it is important to ensure that new technical developments will not hamper the security and intelligence agencies, the use of notices and directions must never be allowed to be a substitute for primary legislation. As the acquisition of bulk communications data by way of section 94 shows, uncertain powers may be used in very broad ways and with little or no transparency. Accordingly, it is appropriate that particular care is taken to put in place very stringent safeguards are in place that will ensure that certainty, clarity and adequate checks are in place for this power.

44. Recommendation 8: As an exceptionally broad and uncertain power that captures matters not expressly foreseen in Parts 1-7:

    (a) National security notices should be subject to judicial authorisation and, in the case of technical capacity notices, approval by the Technical Advisory Board.

    (b) For the avoidance of doubt both national security notices and technical capacity notices should be expressly included in the statistical reporting requirements Cl 174(2)(a)

    (c) Interpretations of the law should be published unless there are exceptional circumstances that require secrecy, in which case publication should be deferred for a maximum period of five years.

45. **Judicial Commissioners – clause 168 – terms and conditions of appointment:** The Bill proposes the use of Judicial Commissioners, rather than judges per se (even though appointees must have prevously held a high judicial office). However, if the Commissioners' safeguarding role is to be effective, is to inspire public confidence and is to be informed by rule of law commitments and the judicial independence that the rule of law requires, then the terms and conditions of appointment should be as close as possible to those which characterise judicial appointments. Of particular concern are:
    - the three-year appointment term under clause 168(2). The Draft Bill is silent on whether this term is renewable; and
    - the dismissal provisions in clause 168(6), with the associated limits in clause 168(4) that do not require parliamentary resolution in 168(6) circumstances.

46. With regard to terms under clause 168(2), it would be appropriate that these be non-renewable fixed terms. It is important that there be absolutely no possibility of perception that a Commissioner's decisions could be influenced by a desire to have a term renewed. The fact that appointment lies in the hands of the Executive, whose decisions the Commissioner will be approving, means that fixed terms are preferable. With the likely office-holders being retired judges, we think it appropriate that an appointee be given an option of taking up a three, four or five year term.

47. With regard to dismissals under clause 168(6), there is insufficient certainty in criterion (a) of "inability or misbehaviour". There is also no certainty in criterion (b) about what the terms and conditions of appointment are and, whatever they will be, we doubt that all terms and conditions should carry equal weight in decisions about removal from office. Again, there must be no possibility of perceptions of opportunities for the

Executive of the Investigatory Powers Commissioner to interfere with independence of individuals or of process. That possibility is alive with such uncertainty, and with the fact that clause 168(4) permits removal from office for inability or misbehaviour without parliamentary resolution. The better path is to require that removal from office on the grounds of inability to carry out the functions of a Commissioner or misbehaviour requires a resolution of each of House of Parliament, except under subsection (5)

48. Recommendation 9: There should be amendments to the appointment and removal processes under clause 168:

    (a) Clause 168(2) should provide for fixed, non-renewable terms of 3, 4 or 5 years, at the election of the appointee.

    (b) Clause 168(4) should remove the reference to subsection (6) and should state that a Judicial Commissioner may not, subject to subection (5), be removed from office except on grounds of inability to carry out the functions of a Commissioner or misbehaviour, and only then not unless with a resolution approving the removal has been passed by each House of Parliament.

    (c) Clause 168(6) should be deleted.

49. **Oversight – clause 171 - notification of serious errors:** The provisions relating to the notification of serious errors are of profound concern. We accept fully that there will be circumstances where a person has suffered significant prejudice or harm but that there will be good reasons (eg, national security) why they should not be notified, and it is right that the legislation provides for that. However, it is entirely inappropriate that the legislative presumption is *against* notification and that the legislation does not provide for notification at a future point when there are no longer reasons for secrecy. The rule of law requires access to justice, and this means that a person who is wronged should have an effective right to a remedy. This is especially so when that wrong has been at the hands of the state, and when the wrong has resulted in significant prejudice or harm.

50. The provision in clause 171(4) stating that the fact there has been a breach of Convention rights will not be sufficient of itself for an error to be a serious error is unnecessary. It is also at odds with the right to an effective remedy under Article 13 ECHR. The provision in clause 171(5)(a) – the Tribunal must consider the seriousness of the error and its effect on the person concerned – is adequate and is to be preferred.

51. Recommendation 10: The legislative provision that allows for non-notification of serious errors should be amended:

    (a) The present presumption in cl 171(2)(b) of non-notification should be reversed, so that where there has been a serious error (being one that has caused significant prejudice or harm) then the person(s) affected will be notified unless it is in the public interest that they are not notified, using the criteria in cl 171(5).

(b) A new sub-section should be inserted providing that, where a person has not been notified on the basis of cl 171(2)(b) then the non-notification is to be reviewed every five years and, if the public interest in non-notification is no longer satisfied then the person is to be notified of the relevant error and the provisions of information should follow cl 171(8).

(c) Clause 171(4) should be removed as it is unnecessary and inconsistent with Article 13 ECHR.

52. **Oversight – annual reporting – clause 174 – statistics on sensitive communications:** The extent to which sensitive confidential communications will be affected by the exercise of powers under the legislation is obviously a matter of public interest. Accordingly, for the avoidance of doubt and with a view to transparency, the legislation should require that the statistical reporting in annual reports include information about those matters.

53. Recommendation 11: Clause 174(2)(a) should be amended to include a requirement that reports identify the number of warrants, etc, that capture or would have captured if issued sensitive communications categories of journalistic sources, legal professional privilege, MPs' communications and other sensitive categories such as medical records and communcications with ministers of religion.

54. **Codes of practice – clause 179 / Schedule 6 - legal professional privilege:** Given the importance of legal professional privilege, its significance for ensuring access to justice and the ability to exercise and protect rights, and the recent admission by the governnent that its policy governing the use of privileged communications was unlawful, in our view it would be appropriate that privilege is dealt with substantially in the body of the statute rather than in the codes of practice.

55. Recommendation 12: The position regarding privileged material should be stated in the body of the statute, rather than being addressed only in the code of practice.

PART 3: CONSOLIDATED LIST OF RECOMMENDATIONS

Power to issue warrants – judicial authorisation rather than 'double lock' procedures

Recommendation 1: Where the 'double-lock' system proposed in the Bill (Parts 2, 3, 5, 6, 7), there should instead be a process in which there is:

- An application by the Secretary of State to a Judicial Commissioner.
- Authorisation should be by Judicial Commissioner, with the test being necessity and proportionality

In the event that that the 'double lock' is retained, the standard for judicial approval should expressly be necessity and proportionality.

It should be noted that all of the following recommendations all still apply even if the 'double-lock' is retained. That is, recommendations 2 - 12 are not dependent on a shift to judicial authorisation

Power to issue warrants, etc – serious crime

Recommendation 2: Serious crime warrants should be on application from law enforcement and made by judicial authorisation.

Power to issue warrants , authorisations or notices – content of an application

Recommendation 3: Applications for warrants (eg, Cl 14(6), 84(6), 107(5), 122(4), 137(4), 153(2), 154(4)) should be required to include:

- an outline of the options for obtaining the relevant data and
- confirmation that other less intrusive options have been tried but failed or have not been tried because they were bound to fail

The same considerations should be required for authorisations (eg, cl 46) and notices (eg, cl 72, 188). In addition, the criteria for warrants, authorisations and notices should always include consideration of whether the information could be reasonably obtained by other means.

Power to issue warrants – urgent circumstances

Recommendation 4: Where an executive warrant or authorisation has been issued in urgent circumstances, judicial authorisation (or approval) should be within 48 hours, rather than five working days (cf. clauses 20, 91, 156, see also cl 119, 147, 160).

Power to issue warrants – clause 61 – journalistic sources

Recommendation 5: Amendments should be made to clause 61:

(a) Cl 61(1)(a): there should be no exception for intelligence services.

(b) Cl 61(1)(a): the safeguards should not apply only when the authorisation is sought 'for the purpose' of identifying or confirming a source, but should apply when it is 'likely' that an authorisation will result in disclosure of a source.

(c) Cl 61(4)(b): this should be reversed so that where there are pre-existing legal representatives for the person to whom the authorisation relates then those representatives must be notified unless there are reasons for not notifying, and criteria for deciding on notification should be set out. Where there is not notification, we recommend the use of Public Interest Special Advocates (see below and Recommendation 6).

(d) Cl 61(7): The definition should be widened so that "source" in clause 61(7) is "any person who provides information to a journalist" and "journalist" is "any natural or legal person who is engaged in the collection and dissemination of information to the public via any means of mass communication".

(e) We also draw attention to recommendation (3) above, which proposes that a part of the PACE model apply generally to the Draft Bill. At the very least, the recommendation (2) provisions should apply to clause 61.

(f) We raise the question of whether protection of the confidentiality of journalistic sources in respect of requests for communications data should also be extended to other established categories of confidential information, i.e. legal professional privilege and communications with Members of Parliament, with doctor-patient confidentiality and communications with ministers of religion also arguably warranting enhanced safeguards.

Power to issue warrants – sensitive confidential communications – inter partes consideration and special advocates

Recommendation 6: We would propose that where a warrant, if issued, would authorise access to sensitive confidential communications (including at least those relating to journalistic sources, MPs communications, and legal professional privilege) then the Judicial Commissioner should be required to make a two-stage decision:

(i) To consider whether an inter partes hearing is viable, including whether it may be viable to notify identifiable legal representatives of a person affected (with undertakings of confidentiality by those lawyers). If an inter partes hearing is viable then the application should proceed on that basis. If a special advocate need to be appointed for part of the hearing then that should occur.

(ii) If an interpartes hearing is not viable then the second stage is proceeded to: then a special advocate should be appointed so that a juducial authorisation is not made in the absence of submissions that would be made if the hearing were inter partes. In recognition of the public interest that underpins the well-established and long-accepted rationales for protections associated with these categories of sensitive communications, and of the importance of hearing submissions on both sides in arriving at a fully informed decision on such important matters, the use of special advocates in these circumstances is appropriate.

Power to issue warrants – novel or especially contentious applications – Special Advocates and open judgments

Recommendation 7: Where an application for a warrant or authorisation is novel or raises especially contentious issues (including the possible interpretation of a statute that would see an expansion of powers that differs from what is apparent on the face of the legislation) then:

(a) a special advocate should be appointed, and

(b) a decision on the legal issues should be published.

National security notices

Recommendation 8: As an exceptionally broad and uncertain power that captures matters not expressly foreseen in Parts 1-7:

(a) National security notices should be subject to judicial authorisation and, in the case of technical capacity notices, approval by the Technical Advisory Board.

(b) For the avoidance of doubt both national security notices and technical capacity notices should be expressly included in the statistical reporting requirements Cl 174(2)(a)

(c) Interpretations of the law should be published unless there are exceptional circumstances that require secrecy, in which case publication should be deferred for a maximum period of five years

Judicial Commissioners – clause 168 – terms and conditions of appointment

Recommendation 9: There should be amendments to the appointment and removal processes under clause 168:

(a) Clause 168(2) should provide for fixed, non-renewable terms of 3, 4 or 5 years, at the election of the appointee

(b) Clause 168(4) should remove the reference to subsection (6) and should state that a Judicial Commissioner may not, subject to subection (5), be removed from office except on grounds of inability to carry out the functions of a Commissioner or misbehaviour, and only then not unless with a resolution approving the removal has been passed by each House of Parliament.

(c) Clause 168(6) should be deleted.

Oversight – clause 171 - notification of relevant errors

Recommendation 10: The legislative provision that allows for non-notification should be amended:

(a) The present presumption in cl 171(2)(b) of non-notification should be reversed, so that where there has been a serious error (being one that has caused significant prejudice or harm) then the person(s) affected will be notified unless it is in the public interest that they are not notified, using the criteria in cl 171(5).

(b) A new subsection should be inserted providing that, where a person has not been notified on the basis of cl 171(2)(b) then the non-notification is to be reviewed every five years and, if the public interest in non-notification is no longer satisfied then the person is to be notified of the relevant error and the provisions of information should follow cl 171(8).

(c) Clause 171(4) should be removed as it is unnecessary and inconsistent with Article 13 ECHR.

Oversight – annual reporting – clause 174 – statistics on sensitive communications

Recommendation 11: Clause 174(2)(a) should be amended to include a requirement that reports identify the number of warrants, etc, that capture or would have captured if issued sensitive communications categories of journalistic sources, legal professional privilege, MPs' communications, and other sensitive categories such as medical records and communcications with ministers of religion.

Codes of practice – clause 179 / Schedule 6 - legal professional privilege

Recommendation 12: The position regarding privileged material should be stated in the body of the statute, rather than being addressed only in the code of practice

19 December 2015

William Binney—written evidence (DIP0009)

My name is William Edward Binney. I am a retired Technical Director of the United States National Security Agency (NSA). I am a United States citizen.

I write to offer to give evidence to your Committee on several aspects of the Draft Investigatory Powers Bill proposals which are, in my judgment and experience and to my knowledge flawed and likely seriously to fail to serve current intelligence and data analysis problems for such purposes as Counter Terrorism. I am willing to travel to the United Kingdom at your invitation.

I conducted and led Signals Intelligence (SIGINT) operations and research for NSA for 36 years. During that time, I served as the lead analyst for strategic warning concerning the Soviet Union/Russia. I was subsequently NSA's Technical Director for World Geopolitical and Military Analysis and Reporting. I have been deeply Involved in solving many technical problems which were coordinated and shared with many SIGINT partners, primarily GCHQ. A fuller CV is appended to this letter.

In 1990, I helped found and then led my agency's SIGINT Automation Research Center. In that capacity, I oversaw the development and construction of the first technologies used for Bulk Collection from Internet communications carried at optical fibre speeds. While working on these technical developments, I started a cooperative technology development among the US, UK and four other European countries. This I viewed as a way to capture target knowledge and leverage technology developments across the group.

In addition to these positions and duties, I was the primary designer and developer of a number of advanced analytic automation programs dealing with complex problems including developing automatic analysis processes for very large amounts of data flowing on the world wide web.

Our experience from the Soviet/Russian problem and in later dealing with terrorism was that to be effective and timely we had to avoid burying our analysts. Our approach was totally different to the historic bulk collect and then word/phrase dictionary select type approach in general use even to this day. In particular, we developed and deployed surveillance tools applying minimisation at the point(s) of collection.

This approach reduces the burden on analysts required to review extremely large quantities of irrelevant material with consequent improvement to operational effectiveness. At the same time, it reduces the privacy burden affecting the large number of innocent and suspicion-free persons whose communications are accessible to our systems.

I have reviewed many NSA documents (released by Edward Snowden and now published) and written since I retired. I note that the problems I helped try to resolve are as grave now as at the start of the information explosion, as indicated by such statements by analysts as:

"Overcome by Overload" "NSA is gathering too much data … impossible to focus"

"Analysis Paralysis" " .. "it's making it difficult for them to find the real threats."

These comments are consistent with my direct experience, which is that bulk data overcollection from Internet and telephony networks undermines security and has consistently resulted in loss of life in my country and elsewhere, from the 9/11 attacks to date.

The net effect of the current approach is that people die first, even if historic records sometimes can provide additional information about the killers (who may be deceased by that time).

The alternative approach based on experience is to use social networks as defined by metadata relationships and some additional rules to smartly select data from the tens of terabytes flowing by. This focused data collected around known targets plus potential developmental targets and represented a much smaller set of content for analysts to look through. This makes the content problem more manageable and optimizes the probability of analysts succeeding.

This approach also has the additional advantage that protected groups can have their communications screened out and excluded from Bulk Collection and analysis, unless a designated and authorised targeting authority is in place. In the United States, under the Constitution, U.S. citizens communications must be excluded when present and detected by NSA systems (again, unless targeting authority is in place).

In respect of the United Kingdom, I have been asked if it was possible for the special protections afforded to Members of Parliament in respect of Interception also to be applied to and maintained in respect of Bulk Collection. The answer, emphatically, is "yes".

To my knowledge and in my experience, such protections from bulk collection could also be applied to other specially protected groups, such as are mentioned in the draft Bill.

I am also able to comment from experience on the risks, management and issues related to bulk and targeted Equipment Interference (also known as Computer Network Exploitation/Computer Network Attack), should the Committee so wish.

I would be happy to discuss any and all of these issues and to provide the Committee with further and/or expanded analysis and proposals.

9 December 2015

William Binney—supplementary written evidence (IPB0161)

1. I gave oral evidence before the Joint Committee on the Draft Investigatory Powers Bill on Wednesday 6 January 2016. I was asked then to answer certain specific questions provided in advance, and also to answer supplementary questions. Some of my answers could not be completed in the time available. I provide the full answers here. I have also been asked to lodge copies of documents provided during the hearing, with explanations.

2. There has been a delay completing this note. I had to travel directly from appearing before the Committee to attend events in California, before returning to the east coast.

Bulk collection and smart collection

3. The proposed legislation presents your Parliament with a great opportunity, I believe, to choose between **Bulk Collection** or **Smart Collection**, thus setting a direction that will have vital ramifications in the future for both your national security and for citizens' human rights.

4. The "Smart Collection" or "Targetted Interception" approach applies intelligence and targeting directly at the point of collection, minimising the retention of data to a manageable, largely meaningful, rich store. The smart collection approach produces actionable intelligence, as evidenced by the retention of critical information on the 9/11 conspirators.

.

5. The bulk collection approach applies no intelligence or targeting at the point of collection, followed by an attempt to sift unmanageable, largely meaningless troves of data through various means including word/phrase dictionary selectors. The bulk collection approach produces up to hundreds of thousands of false positives, burdens analysts, and distracts from the real and critical threats that need prioritising. The problem with bulk collection, aside from eliminating the privacy of the peaceful and law-observant majority of internet users, is that it makes intelligence analysts dysfunctional by drowning them in data. This problem has increased since my time in government service. Numerous of the recent NSA documents released in the last two years refer to analytical staff "overcome by overload" or "drowning in a tsunami of information", and many similar phrases. One member of NSA's in SIGINT directorate wrote as recently as 2011[164] that the "mission is far too vital to unnecessarily expand the haystacks while we search for the needles".

> The SIGINT mission is far too pressing for many team-building activities or brain-storming sessions aiming to improve our organizational approach to analysis. At the same time, the SIGINT mission is far too vital to unnecessarily expand the haystacks while we search for the needles. Prioritization is key.

Those were my own views in 2001.

[164] https://www.documentcloud.org/documents/2088983-too-many-choices.html

6. By doing data acquisition in bulk, your government and my government has permitted what terrorists have wanted all along but could never achieve. That is to cause us to restrict our freedoms while also tripping up our efforts to stop them. Thus, over the last fifteen years, the bulk collection approach has cost lives, including lives in Britain, because it inundates analysts with too much data. It is 99 per cent useless, as attacks occur when intelligence and law enforcement lose focus on previously suspected terrorists and fail to find accomplices or others enabling fresh attacks.

7. This has been the consistent pattern in the U.S. and Europe over the last 15 years. So, people die first, because managers have not proceeded with a professional, disciplined, focused effort. This is the reverse of how they should proceed. Worse, common procedure for most governments after suffering attacks is to request more money, more people and more data - all of which compounds and perpetuates the underlying real problems with the process.

8. Sixteen months before the 2001 attacks on America, our organization inside NSA (Sigint Automation Research Center, or SARC) had invented and was running new methods of finding terrorist networks that worked by using Smart Collection. Our plan was tested and deployed to fields sites, but put aside in favour of a much more expensive plan to collect <u>all communications</u> from everyone. This served the business interests of contractors, but not the American people. Britain may be in the same situation.

9. Subsequent examination of NSA data showed that the 9/11 attacks on the United States could have been prevented if our analysts had filtered relevant data and not attempted to collect everything. Links between the attackers and known terrorist command centers in the Middle East were not noted at the time they occurred, because of data overload. The failure to detect the plans to attack the U.S. was humiliating for the agency. I recommend to that Britain not go further down this road and risk making the same mistakes as my country did, or you will end up perpetuating loss of life.

10. The system we built and deployed was named "Thinthread" within NSA. In addition to its critical national security advantage, the smart collection approach allows agencies to very easily uphold their legal obligations to respect privileged and protected communications, including those of legal and medical professionals, elected representatives, lawyers and others. It also broadly protects the communications data of innocent citizens' from being collected.

11. The replacement U.S. large scale internet surveillance plan, called Trailblazer, also failed to protect my country. It was abandoned after 2005.

12. The Home Secretary's proposals to you involve authorising unrestrained bulk collection by GCHQ, and a complete "internet connection record" of citizens' internet use, including logging everyone who has ever looked at Google, the New York Times, or the BBC, and when they did so. We have known for decades that that type of approach swamps analysts.

13. Information of that kind defeats smart intelligence. For example, it is reasonably likely that everyone in Britain who uses the Internet is linked in two "hops" (connections) to almost every terrorist in the world, because both groups will inevitably have used Google (or the BBC, or Hotmail) at one time or another.

14. The desire to collect everything available is tempting - and doomed on the evidence of the last 15 years. Smart Collection, however, throws away useless and confusing information of that type, enabling resources to be focussed on authorised targets. Such messages may be intercepted, but are never collected or stored.

15. I was concerned when responding to questions in this area that some Committee members may not fully have understood the important operational difference between **bulk interception, bulk collection** and **bulk storage**, and the roles played by **filtering**.

Bulk interception and Lawful Interception (LI)

16. **Bulk Interception** means accessing a high capacity communications system so as to be able to copy all the data it carries. In contrast, **Lawful interception** (a formal term defined by the International Telecommunications Union(ITU)) [165] is limited to copying selected data relating directly to a small set of authorised targets.

17. In **bulk interception**, **filters** are used to control what information passes through and is collected into **bulk storage**, according to prescribed rules.

18. **Filtering** can occur at the point of collection, or during subsequent processing, and also occurs when analysts access bulk storage systems. Filters can be and are applied to exclude material, or to select (include) material. These are fundamentally different processes.

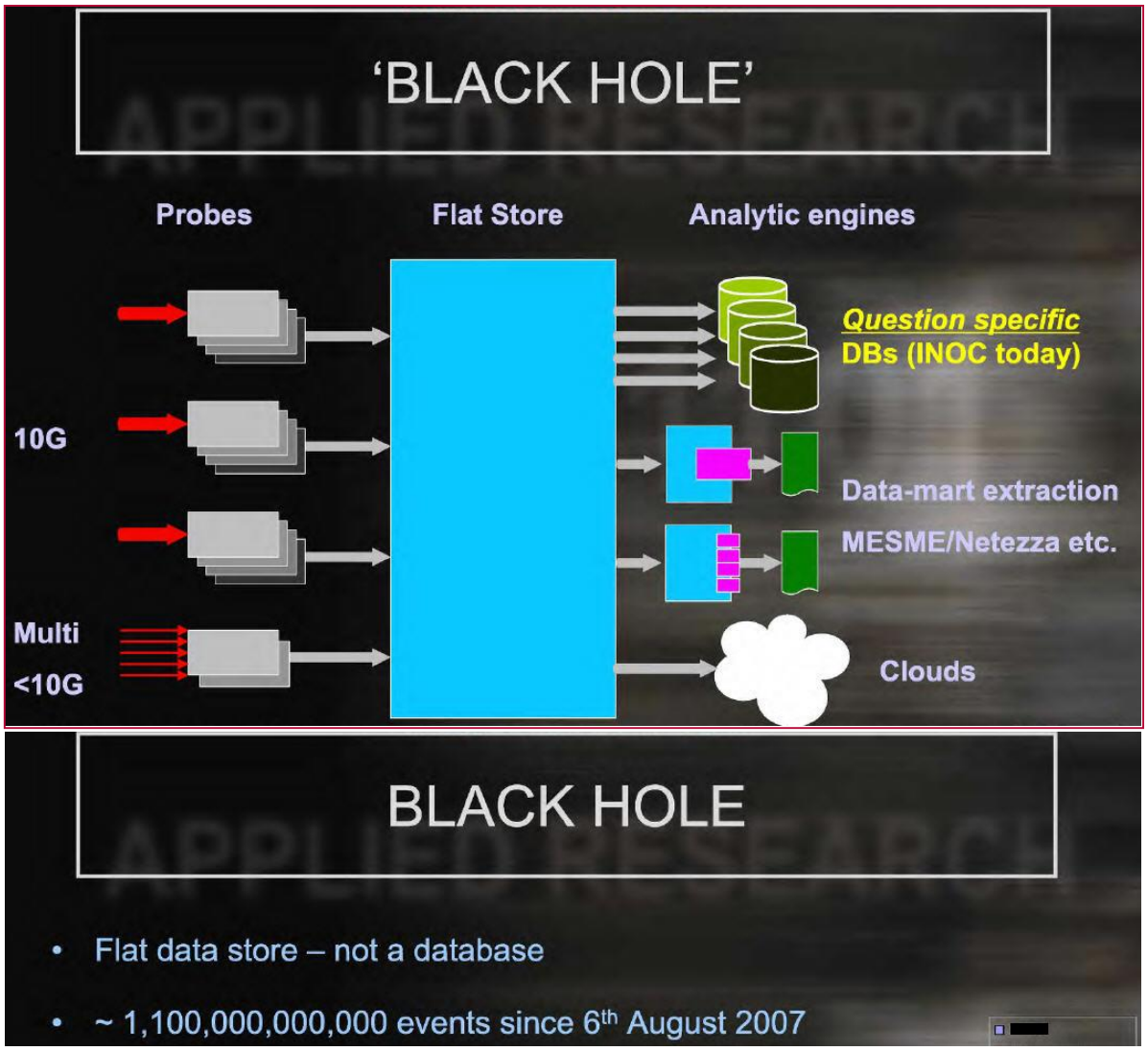
19. Once intercepted data has been through a first filter, it is "collected" (i.e., **bulk collection)** and then passed to storage systems (i.e., **bulk storage**). These are large scale processes now handling of the approximate order of more than 100 billion messages per day in Britain, and perhaps 50 times that for NSA.

20. Currently, the first or "front end" filters used by GCHQ and NSA are in simple terms rubbish filters. They are not Smart Collection filters as described here. I have been told that GCHQ has claimed already to use the methods I describe here, by selecting at the point of collection. That understanding is entirely wrong, to my knowledge and according to published descriptions of GCHQ's Tempora system. Rubbish filters do remove items such as spam e-mail, and streaming published video which has no intelligence significance. They pass on, or "ingest" all the rest.

165 www.itu.int/dms_pub/itu-t/oth/23/01/t23010000060001mswe.doc

21. GCHQ documents specifically state that it retains all personal and organisational information including " webmail, email, transfers, ftp, chat, internet browsing, website logins, vbulletin, web fora, web cams, gaming, social networking -- and the list is growing." [166]

22. I have noted the evidence given to the committee concerning disclosed plans for the GCHQ Internet surveillance system called BLACK HOLE, which has operated since 2007. It attempts to list everyone who has been to any website on the Internet, and many other tasks. (Every day, according to the published GCHQ documents, BLACK HOLE collects about a thousand records for every person living in the UK. (64 billion).[167]



Extracts from GCHQ Applied Research report on "QFDs and BLACKHOLE"

23. The way data is gathered by GCHQ and NSA probes is shown in the diagrams above. The rubbish filter is applied at the cable Probes (connectors, far left) before data is

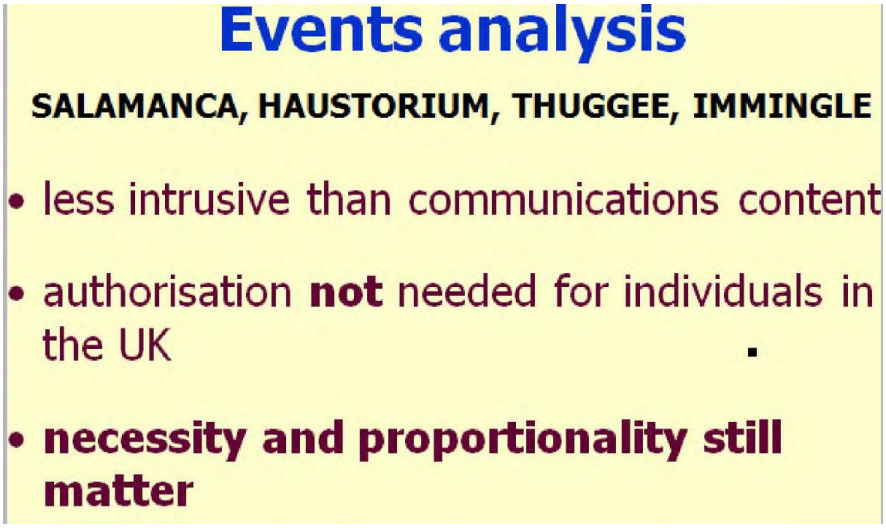
166 https://www.eff.org/files/2015/10/12/20150925-intercept-data_stored_in_black_hole.pdf

167 http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/26382.pdf

sent (grey arrows) to the "flat store" (centre). The data is retained in the store but can be analysed and filtered in response to analysts' queries. In the language used in the draft Bill, this would be a "request filter". All the bulk data collected is retained, even if not queried, and remains available to all other queries, from any source.

24. The scale of the GCHQ Black Hole system by 2009 shown in the published document (above) was in excess of one trillion (million, million) records. We used many similar bulk storage systems at NSA.

25. The data intercepted, collected and stores comes from all countries. It is clear from these published documents that GCHQ, like NSA, stores "Events" data or metadata on all persons seen in data, including their own citizens. Authorisation for individuals in the UK is stated by GCHQ to be "not needed", as shown in the diagram below. [168]



26. GCHQ and NSA both use the operational term "**defeat**" to described specific filtering methods to prevent data being stored. "Defeats" specify targets or their communications systems whose data should not be stored. These can easily included countries or personalities ordered not to be targetted, such as lawyers, medical staff, or elected representatives.

27. Regards international comparisons, as you, the authorisation of section 215 of the PATRIOT Act, allowing for bulk data collection from telephony networks, was revoked in June 2015. There are ongoing legal challenges on the matter in the US. There are legal challenges to bulk data collection in Europe also. I would suggest that the continuation of bulk data collection in coming years will become untenable, given that operational inefficiency will be increased by the scale of overcollection.

Legal and parliamentary privilege

28. The government has misled Parliament about protecting members of Parliament or other important sensitive professions from mass surveillance by bulk collection. This is

168 https://archive.org/details/master-current-20081127

exceedingly simple to do. I recommend you suggest new language for your law, which requires intelligence agencies to apply minimisation to bulk collection, using "defeats".

29. My attention has been drawn to claims by UK government lawyers to the Investigatory Powers Tribunal (IPT) that "there is so much data flowing along the pipe" [optical fiber cables] that data "isn't intelligible at the point of interception". These claims are false. "They were made by someone who does not understand the technology. IPT members were misled.

30. The solution is to do a focused disciplined professional selection of meaningful data from the flow of information going around the world. This is the better alternative to bulk collection.

Simple guide to filtering

31. For the further assistance of the Committee, I attach diagrams as an Annex.

32. Communications networks are operated by machines (routers and servers) and software. These machines are programmed to move data around the world.

33. To acquire information off the fibers, you first need to know where all these fiber lines converge. You need to know the points of convergence of these lines to determine where to tap and get the most output from your collection investment. That is, if you place a collection set of equipment at a fiber convergent point you optimized data collection results as the equipment will be able to see multiple lines simultaneously. And, if you cover most of the converging points, you have the opportunity to collect most of the data on the worldwide network.

34. The machines use metadata (phone numbers, IP addresses…) to move information. This metadata is organized in unique worldwide systems that divide the world into regions. For the phone network, the system includes nine regions of the world and is managed by the ITU (international telecommunications Union) and includes fixed landline, mobile cell and satellite phones (slide 2).

35. In a similar way, the internet is numbered with IP (IPV 4 and IPV 6). Numbers and machine access codes (MAC) plus user name/service attributes are used to route communications. In this system the world is divided into five Regions (slide 3).

36. The data is used to build social networks and also show patterns of interactions within these networks as well as physically tracking them (slides 4 to 6). These slides give examples of social network reconstruction or contact chaining/ network reconstruction. This enables detection of bad actors without unreasonably violating privacy.

37. First you use the knowledge of known bad actors then use network relationships to restrict the collection of data to a zone of suspicion around bad actors. This makes content a manageable problem for analysts to handle and allows them to succeed at their studies.

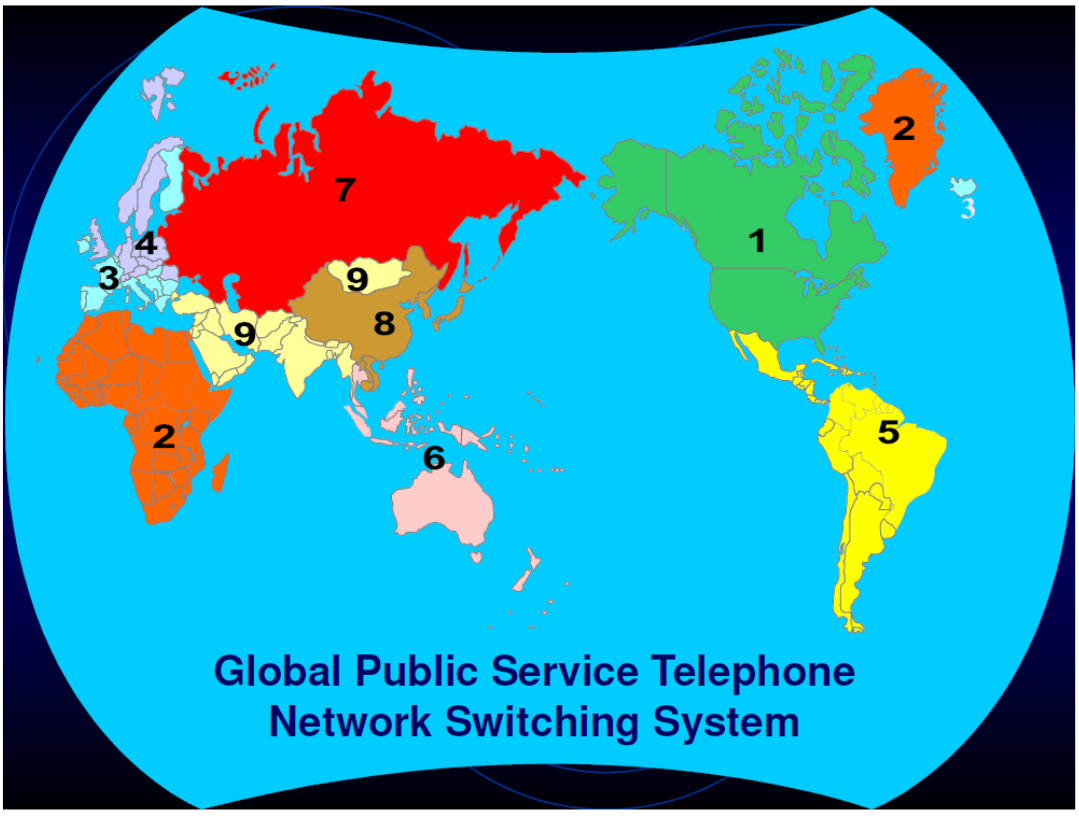
38. Recognition of important information detected in smart selection should be automatically alerted to all concerned using verified rules for distribution.

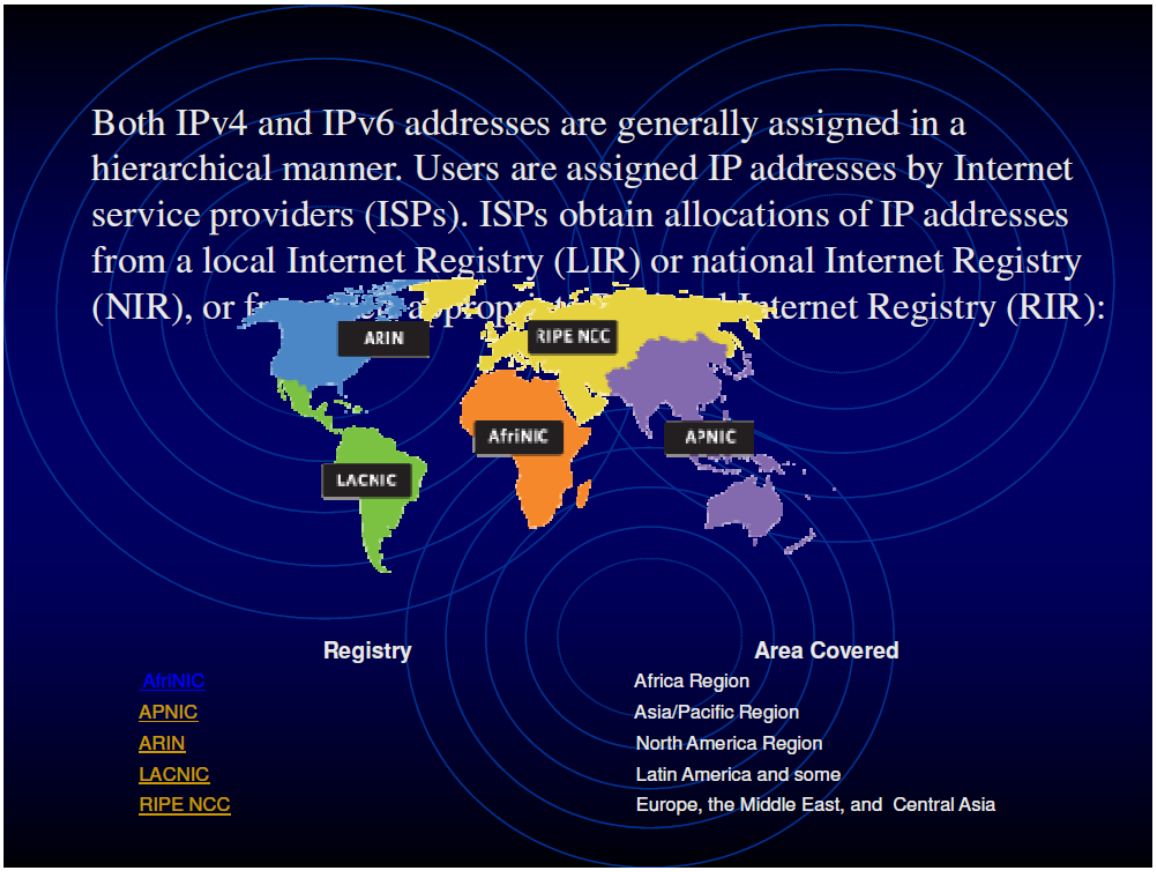
39. If necessary, even the court process of issuing warrants could be automated providing an agreed criteria is used to request and authorize warrants.

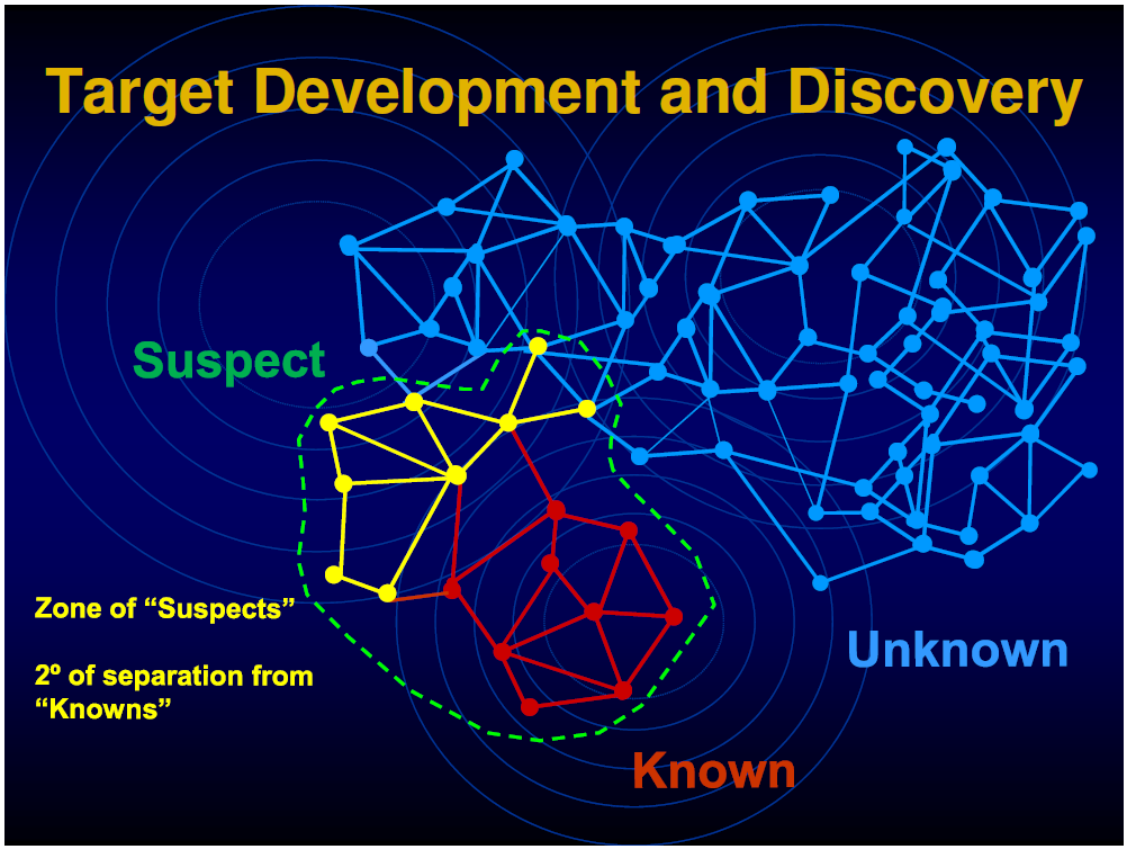
40. Slide 6 shows the actual pattern of open source reported connections recorded prior to the 9/11 attacks, and conclusively linking attack planners to the suicide team already in the US. Because of overcollection, these links were not seen until after the attack had taken place.

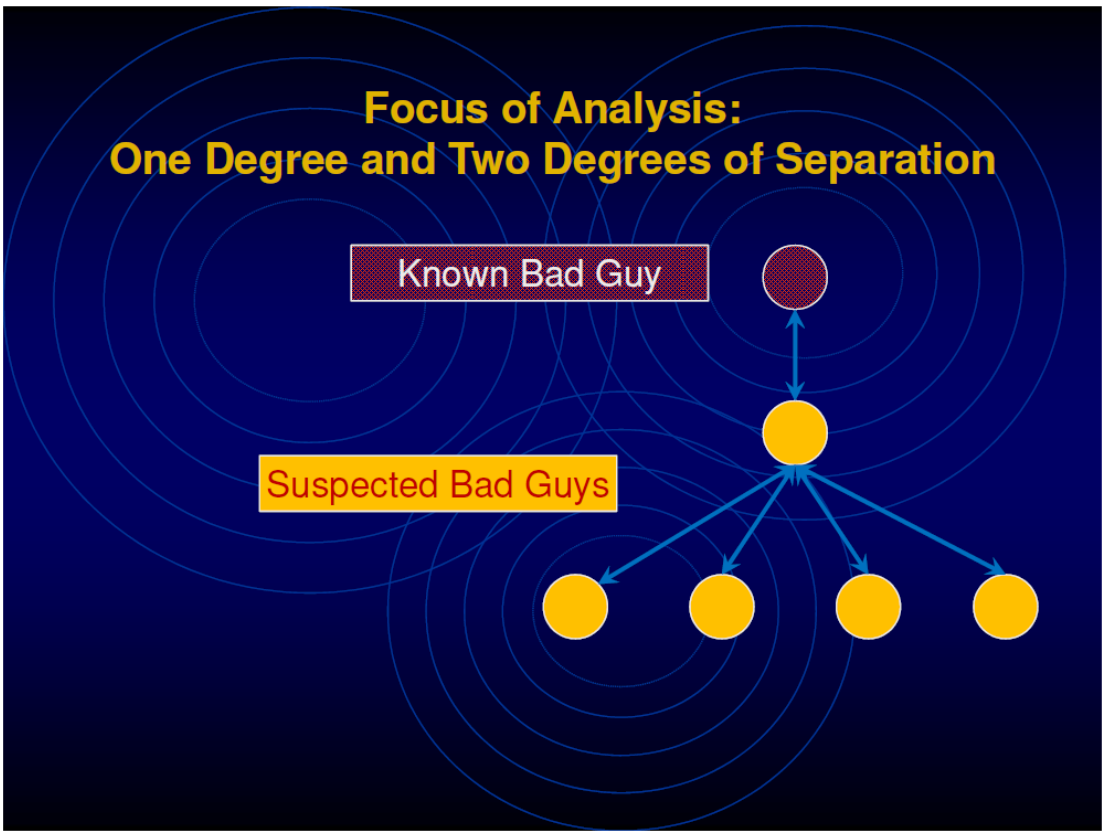
Attached: Annex (5 slides)


Mass Surveillance
William Binney
Former Technical Director at NSA


7
4
3
9
9
8
2
6
2
1
3
5
Global Public Service Telephone
Network Switching System


Both IPv4 and IPv6 addresses are generally assigned in a hierarchical manner. Users are assigned IP addresses by Internet service providers (ISPs). ISPs obtain allocations of IP addresses from a local Internet Registry (LIR) or national Internet Registry (NIR), or f
ternet Registry (RIR):
ARIN
RIPE NCC
AfriNIC
APNIC
LACNIC
Registry
Area Covered
AfriNIC
APNIC
ARIN
LACNIC
RIPE NCC
Africa Region
Asia/Pacific Region
North America Region
Latin America and some
Europe, the Middle East, and Central Asia


Target Development and Discovery
Suspect
Zone of "Suspects"
2º of separation from "Knowns"
Unknown
Known



12 January 2016

Brass Horn Communications—written evidence (IPB0067)

This submission is written on behalf of Brass Horn Communications, a small, membership orientated, volunteer run, non profit Internet Service Provider based in the United Kingdom which also operates one of the larger UK based Tor relay families.

Bulk interception and bulk retention of "Internet Connection Records" will not be as useful as the Home Office are claiming them to be and will instead be treating every UK citizen as a suspected criminal. Those of interest to the Investigatory Powers Bill will likely protect their communications and their meta-data. As privacy becomes a commodity companies and community software will take more steps to protect people from the prying eyes of criminals and the state.

Pages 2 to 5 discuss how the use of Tor (https://www.torproject.org/) would render many aspects of an Internet Connection Record useless for ascertaining the destination, content or meta data of a communication.

Page 5 also discusses how ICRs could be contaminated by malicious actors or the background noise of the Internet.

Page 6 discusses whether forcing entities subject to the powers in the Draft Investigatory Powers bill to remain silent *(or in the case of an existing warrant canary; forcing them to lie to their customers)* and ICR retention are necessary.

Appendix A delves into what an Internet Connection Record *could* be (the definition is fuzzy at best) and then through a series of worked examples which expose the issues with ICRs.

Appendix B tackles the idea discussed at 17:34 during the oral evidence session on November 30th 2015 where a CSP could be compelled to remove the electronic protection of a message and that many of the companies have control as to whether users choose to encrypt their messages end-to-end.

Appendix C provides an overview of how Tor works.

Are The Powers Sought Workable?
Defeating ICR Retention
1. The oral evidence given at ~18:18 on the 30th of November 2015 discussed how Internet Connection Records (ICR) would ensure that law enforcement could 'close the gap' regarding the capability to identify who someone was or what other CSP they were communicating with.

2. Mass retention of ICRs would be rendered mostly useless if a person was using Tor, a VPN or other tunnelling technology to conceal which endpoints they were communicating with. Appendix C discusses how Tor works in more detail.

3. Section 71(9) of the draft bill defines relevant data that may be used to identify or assist in identifying any of the following;

10. the sender or recipient of a communication (whether or not a person),
11. the time or duration of a communication,
12. the type, method or pattern, or fact, of communication,
13. the telecommunication system (or any part of it) from, to or through which, or by means of which, a communication is or may be transmitted,
14. the location of any such system, or
15. the internet protocol address, or other identifier, of any apparatus to which a communication is transmitted for the purpose of obtaining access to, or running, a computer file or computer program.

4. Taking the common example of Alice and Bob[169]; Alice wants to visit Bobs website (www.website.bob) and read the page www.website.bob/search/bomb, if Alice were to visit the website over an unprotected, retained connection her ICR would be *(assuming the technical capability to capture and resolve all information, see appendix A)* as follows;

s.71(9)(a)	IP address 192.0.2.10 is currently allocated to Alice
s.71(9)(b)	01/12/2015 13:00 (no duration yet as this is the first packet sent)
s.71(9)(c)	A HTTP GET for the page /search/bomb of domain www.website.bob with a source TCP port of 4895 to and a destination TCP port of 80
s.71(9)(d)	Mobile phone network, 3G
s.71(9)(e)	The CSP will have to look up which tower(s) Alice's phone is nearby and store that information
s.71(9)(f)	Bob's server's IP address is 198.51.100.100

Figure #1

However if Alice was to use Tor then the ICR would have been;

s.71(9)(a)	IP address 192.0.2.10 is currently allocated to Alice
s.71(9)(b)	01/12/2015 13:00 (no duration yet as this is the first packet sent)
s.71(9)(c)	The connection is encrypted so all the CSP can record is the source port (tcp/4895) and destination port (tcp/**9200**) (and the fact it is encrypted via Tor)
s.71(9)(d)	Mobile phone network, 3G
s.71(9)(e)	The CSP will have to look up which tower(s) Alice's phone is nearby and store that information
s.71(9)(f)	The Tor relay's IP address is 203.0.113.100

Figure #2

5. Note how Alice's ICR shows her making a connection to the Tor relay and **not** to Bobs website.

[169]https://en.wikipedia.org/wiki/Alice_and_Bob#Cast_of_characters

6. In fact if Alice were to use Tor as her normal transit protection then **all** of her ICR records would be encrypted and no meta data *(beyond knowing she was using Tor)* would be collectible.

7. As a Tor relay operator it is possible that during the course of an investigation the Home Office may choose to serve a retention warrant against us170 in order to expose Alice and Bobs communications.

8. Thankfully, due to the design of Tor even if the state had retention records of Alice's ISP and of our Tor relays the records would still be quite sparse *(doubly so if Bob offered his website over HTTPS);*

Step	**Alice's ISP ICR**	**Brass Horn Comms ICR**
1. Alice connects to a Tor relay in Spain	Encrypted connection to a Spanish Tor relay	
2. Alice connects to the next 'hop' relay in the US	Encrypted connection to a Spanish Tor relay	
3. Alice connects to the Brass Horn Comms exit relay	Encrypted connection to a Spanish Tor relay	An encrypted connection from the US 'hop' relay *(note we don't "know" about the Spanish relay or Alice)*
4. Alice requests https://www.website.bob/test	Encrypted connection to a Spanish Tor relay	An encrypted connection from the US 'hop' relay requesting https://website.bob *(note we don't see /test)*
5. Alice changes the middle hop to a relay in Russia	Encrypted connection to the Spanish Tor relay	
6. Alice requests https://www.website.bob/search/bomb	**Still** just an encrypted connection to the Spanish Tor relay	An encrypted connection from the **Russian** 'hop' relay requesting https://website.bob *(note we don't see /search/bomb and we still don't "know"about the Spanish relay or about Alice)*

Figure #3

9. Looking at this as a (simplified) IP packet shows the situation more clearly.

Alice's IP address:	**192.0.2.10**
Bob's website IP address:	**198.51.100.100**
Bob's website TCP port:	**80**

[170]We do not currently retain *any* data and are therefore unable to comply with any retention notice due to the fact it is not an extension of existing capability. (We would also work to refuse any such warrant).

10. Alice's request over an unprotected retained connection:

Src Addr: 192.0.2.10	Src Port: 4895
Dst Addr: 198.51.100.100	Dst Port: 80
Time: 01/12/2015 13:00:00	
Data: HOST: www.website.bob GET: /search/bomb	

Figure #4

11. Bob's Server's Reply to Alice's request over an unprotected retained connection:

Src Addr: 198.51.100.100	Src Port: 80
Dst Addr: 192.0.2.10	Dst Port: 4895
Time: 01/12/2015 13:00:01	
Data: <!HTML><title>Bob's website</title><body>These	are bobs bomb instructions....</body>

Figure #5

12. This is now very different if Alice was using Tor.

Alice's IP address:	**192.0.2.10**
Bob's website IP address:	**198.51.100.100**
Bob's website TCP port:	**443**
Spanish Tor Relay:	**203.0.113.100**
Russian Tor Relay:	**203.0.113.200**
Brass Horn Communications Tor Exit:	**203.0.113.250**

13. Alice's request to Bob's website over a Tor connection:

Src Addr: 192.0.2.10	Src Port: 4895
Dst Addr: 203.0.113.100	Dst Port: 9200
Time: 01/12/2015 13:00:00	
Data: **<encrypted>**	

Figure #6

14. The reply to Alice's request via Tor:

```
+-----------------------------------------------------+
| Src Addr: 203.0.113.100  | Src Port: 9200           |
|-----------------------------------------------------|
| Dst Addr: 192.0.2.10     | Dst Port: 4895           |
|-----------------------------------------------------|
| Time: 01/12/2015 13:00:20                           |
|-----------------------------------------------------|
| Data: <encrypted>                                   |
+-----------------------------------------------------+
```

Figure #7

15. Note how the ICR record makes no mention of Bobs server IP, the Russian Tor relay or the Brass Horn Communications Tor Exit relay.

16. There is no way to know if Alice is communicating using HTTP with Bob's server, a Facebook server or a Twitter server. These ICRs couldn't tell if she is communicating via XMPP to an instant messaging platform, via SSH to her own server or all of these at the same time.

17. As more people become aware of the need to protect their communications from eavesdroppers *(be it criminals or the state)* then ICRs will become less and less useful.

18. The popular web browser Mozilla Firefox is considering deploying a Tor feature to their browser171 which will mean that upwards of ~11% of web browsing in the United Kingdom is likely to be obfuscated in the manner described above **with no additional action required by the user**.

19. Whilst Brass Horn Communications is based here in the UK a significant number of Tor relays are in countries outside the jurisdiction of the Draft Investigatory Powers Bill meaning that ICRs will be of dwindling use as more people defend themselves against mass surveillance.

Poisoning ICR Retention

20. If, for example, the *People's Front of Judea* maintained a website and the state was monitoring any connection to the website / IP address 203.0.113.200 then it would be dangerous for anyone *(a journalist, a curious citizen etc)* to visit this website as they could then be tagged as a person of interest *(e.g. NSA Keyscore targeting anyone who visited the Linux Journal website172).*

21. One way the *People's Front of Judea* could waste state resources would be to compromise innocent websites or an advertisement network to include a small piece of HTML code to fetch data from the server thereby creating an ICR linking the user to the *People's Front of Judea*.

[171]https://blog.torproject.org/blog/partnering-mozilla

[172] http://www.theregister.co.uk/2014/07/03/nsa_xkeyscore_stasi_scandal/

22. The code could be as simple as;

23. This could render an image only 1 pixel in size *(assuming the image was in fact 1x1 pixels big)* on the users screen without their knowledge.

24. If the image was fetched over HTTPS then the ICR would only show that people were connecting to the *People's Front of Judea* website but would not know what data they were sending or receiving *(granted the data volumes would be tiny in this example but resources may still be wasted investigating why so many ICRs were showing activity to the People's Front of Judea website).*

25. As discussed further in Appendix A any IP address on the Internet is likely to receive a lot of unsolicited traffic from port scans, malicious exploitation attempts by viruses or botnets, simple mistakes or in some cases huge amounts of traffic in an attack known as a Distributed Denial of Service (*the attack overwhelms a node by virtue of the sheer amount of traffic directed at it thereby "denying service" to the owner).*

Are the Powers Sought Necessary?

Gagging Notices

26. During the oral evidence on November 30th 2015 at 17:27 the question was asked as to whether the Draft Investigatory Powers Bill would put UK CSPs at a disadvantage to businesses who were not subject to retention and interception powers. The question was dismissed as a commercial issue or that the powers are not new but this is not the case; various people only choose to use a CSP that guarantees the protection of their communications.

27. Some members of Brass Horn Communications and many members of the global community only use our services as we publish what is known as a warrant canary[173] which is a way of communicating that one has not been subject to *(and are not otherwise co-operating with)* a UK data retention warrant or a US national security letter etc.

28. By preventing niche CSPs from being able to effectively communicate these facts [s77(2)] they will almost certainly lose customers as well as losing the trust and good standing within the various communities in which they operate.

29. It is quite possible that vulnerable people here in the UK who rely on our Tor relays will no longer be able to trust them and would instead have to use others that may be geographically distant *(reducing effective performance)* or otherwise possibly unsafe *(e.g. operated by an unscrupulous entity intent on stealing credentials that egress their nodes in plain text such as criminals, the FBI etc)*.

[173] https://brasshorncommunications.uk/canary/

30. I understand from the notes published at http://www.revk.uk/2015/11/home-office-ipbill.html that it was the large incumbent ISPs that requested these gagging clauses. Let us not forget that it is these same incumbents who;

6. Assisted with the unpopular mass surveillance exposed by Edward Snowden and such gagging orders provide them with plausible deniability **whilst removing a competitive edge from smaller / niche CSPs**
7. Have been found to intercept and retain their customers browsing habits to sell to advertising agencies174
8. Deployed DPI equipment to intercept, profile and block customer traffic175

31. Gagging notices are a form of suppression and are not necessary.

Mass/Bulk Retention

32. Mass (Bulk) retention of innocent peoples web browsing has been found to be a violation of human rights.

33. We've shown in this evidence that ICRs can be defeated by those of potential interest to the bill and as privacy becomes more important to the general populace even the 'emotional' examples the NCA likes to use (e.g. missing children) will be thwarted by improved privacy technology.

34. Mass/Bulk retention of Internet records is excessive, intrusive and not necessary.

Appendix A – What is an Internet Connection Record?

Section 71(9) provides the closest definition of what an Internet Connection Record is but it is not a type of record that CSPs routinely record.

Most communication over the Internet is built on top of the Internet Protocol as defined in RFC 791176. Any given IP packet will have a source address and a destination address as detailed in Figure 4 of RFC 791 *(copied below for convenience)* which would comprise the elements requested in s.71(9)(a), s.71(9)(f);

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|  IHL  |Type of Service|          Total Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Identification          |Flags|      Fragment Offset    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Time to Live  |    Protocol   |         Header Checksum       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Source Address                                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               Destination Address                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               Options                         |    Padding    |
```

[174] http://www.telegraph.co.uk/technology/news/8438461/BT-and-Phorm-how-an-online-privacy-scandal-unfolded.html
[175] https://nodpi.org/2010/08/07/talktalk-becomes-stalkstalk/
[176] http://tools.ietf.org/html/rfc791

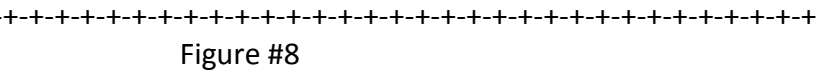


Figure #8

Common protocols such as HTTP *(used for web browsing)* rely on TCP177 to ensure reliable communication between two hosts. A TCP packet looks similar to the IP packet seen earlier but adds additional information of relevance to s.71(9)(c) such as the source port *(e.g. TCP port 80 would commonly dictate a web server, TCP port 443 a secure web server (HTTPS) etc);*

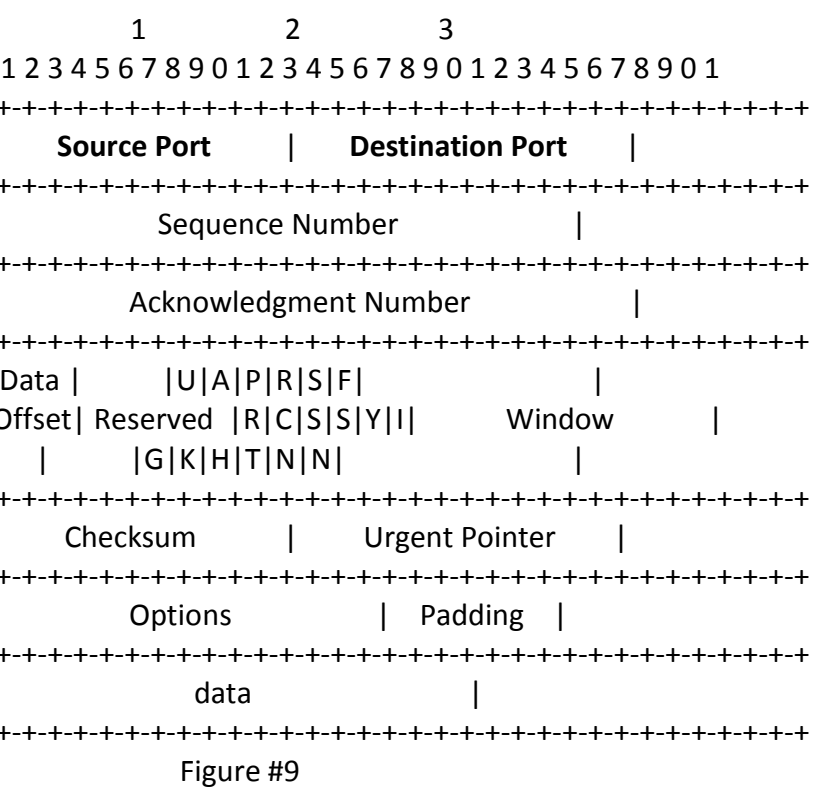


Figure #9

Only 50% of the requirements specified in s.71(9) are contained in a TCP/IP packet, to gather the information required in s.71(9)(c), s.71(9)(e) would require extracting information from the 'data' part of a TCP packet which requires the individual packets be reconstructed and then processed. This practise is commonly referred to as “Deep Packet Inspection” (DPI), unfortunately for the Investigatory Powers Draft DPI is usually defeated by transport encryption such as TLS.

Example #1

Problems occur when a CSP tries to follow the spirit of the requirements, take for example a TLS secured WebSocket178 connection;

Alice's phone initiates an encrypted handshake with a server on Tuesday 1st December 2015 at 13:00

s.71(9)(a)	Alice's IP address is 192.0.2.10
s.71(9)(b)	01/12/2015 13:00 (no duration yet as this is the first packet sent)

[177]http://tools.ietf.org/html/rfc793

[178]https://www.rfc-editor.org/rfc/rfc6455.txt

s.71(9)(c)	The connection is encrypted so all the CSP can record is the source port (tcp/4900) and destination ports (tcp/8080) (and the fact it is encrypted)
s.71(9)(d)	Mobile phone network
s.71(9)(e)	The CSP will have to look up which tower(s) Alice's phone is nearby and store that information
s.71(9)(f)	The server's IP address is 192.0.2.20

Figure #10

The handshake completes after a few packets back and forth containing no additional information.

No further data is received.

5 minutes later A single TCP packet with a data payload of a few bytes *(e.g. the encrypted form of a single ASCII character)* is sent from 192.0.2.20:8080 to 192.0.2.10:4900 and a TCP/ACK is sent from Alice's phone to the server. Is this part of the original communication *(in which case the original ICR needs to be updated to have a 'duration' of 5 minutes)* or is it a new ICR?

50 minutes later a burst of 50 kilobytes of traffic is sent from 192.0.2.20:8080 to 192.0.2.10:4900. This pattern will continue for some weeks but 9 minutes after this burst of traffic a packet is sent from 192.0.2.30:8080 to 192.0.2.10:4900 *(note the last octet is 30 not 20),* Alice's phone sends a TCP/NACK (rejecting the message). This was an unsolicited message, does it count against Alice's ICR? If 192.0.2.30 is an IP address known to be used by criminals is Alice now implicated?

15 minutes later Alice is the victim of a Distributed Denial of Service attack as several tens of thousands of IP addresses send a single packet to TCP port 4500 on Alice's phone, 5 seconds later they do it again, 6 seconds later tens of thousands of different IP addresses send a single packet to Alice's phone. Is each of these is a new connection to be recorded as an ICR?

13 months later Alice's phone receives a burst of data from 192.0.2.20:8080. Is this part of the original communication or a new communication where the original ICR retained handshake was lost? The original record is lost as it is over 12 months old so what should be done?

Example #2
In this example Charlie179 is browsing a website from home. His browser makes an encrypted request to https://192.0.2.20 at 14:00 on the 1st of December 2015

s.71(9)(a)	The CSP records that Charlies home modem was assigned 192.0.2.70
s.71(9)(b)	01/12/2015 14:00 (no duration yet as this is the first packet sent)
s.71(9)(c)	The connection is encrypted so all the CSP can record is the source port (tcp/43245) and destination ports (tcp/443) (and the fact it is encrypted)
s.71(9)(d)	The CSPs infrastructure

[179]https://en.wikipedia.org/wiki/Alice_and_Bob#Cast_of_characters

s.71(9)(e)	This record pertains to Charlie so the CSP could look up their billing / service address
s.71(9)(f)	The server's IP address is 192.0.2.20

Figure #11

Each image and stylesheet on the website might result in different connections to Content Delivery Networks such as Akamai, are these requests related to this ICR or are they an ICR in their own right?

The web page finishes loading and Charlie starts reading it. He sees a link and clicks it. A whole new HTTPS and TCP session starts even though Charlie is just reading a different page on the same website

s.71(9)(a)	The CSP records that Charlies home modem was assigned 192.0.2.70
s.71(9)(b)	01/12/2015 14:05 (is the duration 5minutes or is this a new ICR?)
s.71(9)(c)	The connection is encrypted so all the CSP can record is the source port (tcp/**23089**) and destination ports (tcp/443) (and the fact it is encrypted)
s.71(9)(d)	The CSPs infrastructure
s.71(9)(e)	This record pertains to Charlie so the CSP could look up their billing / service address
s.71(9)(f)	The server's IP address is 192.0.2.20

Figure #11

Note how Charlies browser has chosen a new source TCP port to receive the information back from the server. Is this a new ICR or simply a browsing session that has lasted 5 minutes?

Charlie goes off to make a cup of tea and comes back to his computer 15 minutes later. He clicks another link. Again, a new HTTPS and TCP session starts but this time his computer co-incidentally chooses port 43245 again to listen to the response from the server.

Is this a new ICR or is Charlie's original web browsing ICR now 20 minutes long?

This might not seem important but if a case was being built against Charlie would two cursory (~5 seconds) visits to a criminal website 20 minutes apart be looked upon differently to a 20 minute long “session”?

Appendix B – A Note on End to End Encryption

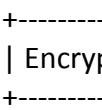
End to End Encryption

We saw from the oral evidence on November 30th that there is awareness of end-to-end encryption however there is an oft repeated assumption that all end-to-end encryption is controlled by commercial entities.

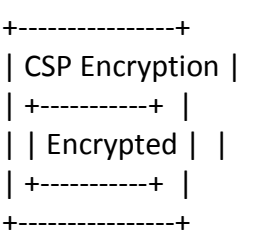
There are many over-the-top (OTT) encryption possibilities that allows an individual to encrypt their messages without any action from the CSP over whose service the resulting message is sent.

We can take an example of Alice and Bob180 who wish to communicate privately. Bob is currently under targeted surveillance and Alice is a journalist, for reasons of this example they are using a CSP who has been instructed to retain data and remove any “electronic protection”

Alice encrypts her message with a key that only Bob knows;



She then sends this message via the CSP who wraps it in another layer of encryption



The Police have a copy of this message and instructs the CSP to remove the electronic protection *(highlighted in blue)* but is simply left with the original message which **is still encrypted.** There is nothing the CSP can do to remove this additional layer of protection.

The situation becomes more complex when we start to consider the free and open source software communities (FOSS). FOSS communities build software that is not encumbered by a closed license terms and does not need to be purchased. The source code for this software is available for anyone to read and change to make their own versions from.

A loose knit, global community of users could decide to build a WhatsApp or iMessage clone that provides user supplied end-to-end encryption with no central server infrastructure. There would be no CSP to serve a warrant to, no servers to perform interference on. As people learn that this free software protects their rights **and** protects their communications they may well transition their communications to this new software *(we recently saw millions of people in Brazil switch from WhatsApp to Viber and Telegram in just a few days when Brazil blocked WhatsApp)*.

The technical community will build surveillance frustrating technology as there is the need and desire for privacy and security; people are acutely aware that there is a chance that a programme such as GCHQ's “Degrade, Deceive, Discredit” could be misused in the way that France's emergency terrorism powers have been used against Climate protesters181 or the Metropolitan Police's Special Demonstration Squad used their undercover powers to manipulate relationships.

Appendix C – How Tor (The Onion Router) Works

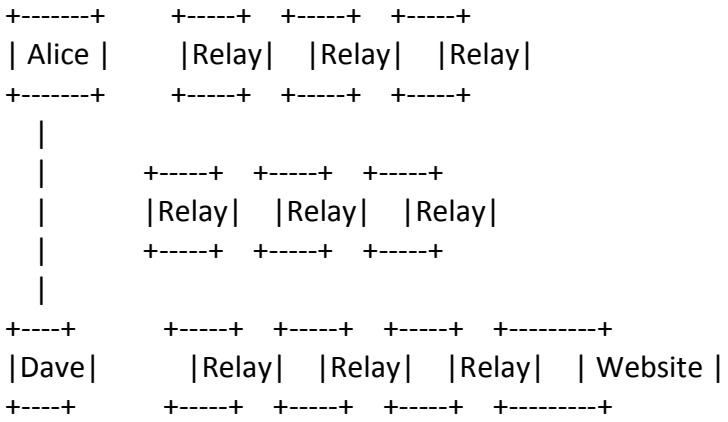
Tor Operation

[180]https://en.wikipedia.org/wiki/Alice_and_Bob#Cast_of_characters

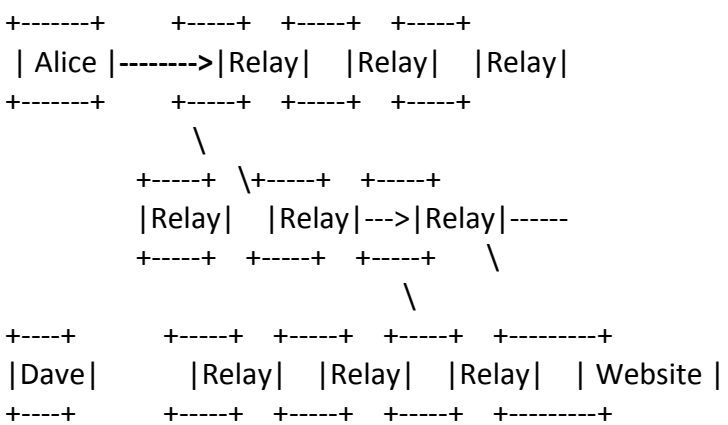
[181]http://www.theguardian.com/environment/2015/nov/27/paris-climate-activists-put-under-house-arrest-using-emergency-laws

The Tor network is a group of volunteer-operated servers that allows people to improve their privacy and security on the Internet. Tor's users employ this network by connecting through a series of virtual tunnels rather than making a direct connection, thus allowing both organizations and individuals to share information over public networks without compromising their privacy.

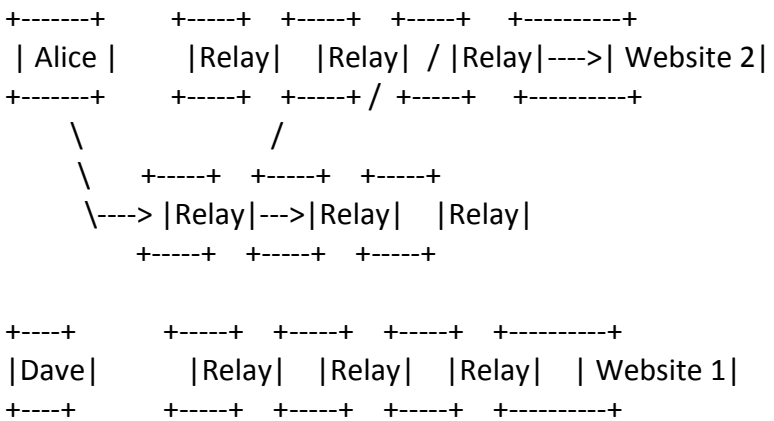
Step 1:
Alice's computer acquires a list of Tor relays from a directory server (in this case Dave's server)



Step 2:
Alice's Tor client picks a random path to a destination server.



Step 3:
If at a later time Alice visits a different website her Tor client will select another (different) random path.



Tor helps to reduce the risks of both simple and sophisticated traffic analysis by distributing transactions over several places on the Internet, so no single point can link Alice to her destination.

The idea is similar to using a twisty, hard-to-follow route in order to throw off somebody who is tailing you — and then periodically erasing your footprints. Instead of taking a direct route from source to destination, data packets on the Tor network take a random pathway through several relays that cover your tracks so no observer at any single point can tell where the data came from or where it's going.

To create a private network pathway with Tor, the user's software or client incrementally builds a circuit of encrypted connections through relays on the network. The circuit is extended one hop at a time, and each relay along the way knows only which relay gave it data and which relay it is giving data to. No individual relay ever knows the complete path that a data packet has taken. The client negotiates a separate set of encryption keys for each hop along the circuit to ensure that each hop can't trace these connections as they pass through.

Once a circuit has been established, many kinds of data can be exchanged and several different sorts of software applications can be deployed over the Tor network. Because each relay sees no more than one hop in the circuit, neither an eavesdropper nor a compromised relay can use traffic analysis to link the connection's source and destination.

20 December 2015

BT—supplementary written evidence (IPB0151)

1. Introduction

BT welcomes the Joint Parliamentary Committee's call for evidence on the draft Investigatory Powers Bill (IPB).

Publication of the IPB means that, for the first time, there is one document that sets out the totality of investigatory powers that Government considers necessary in relation to communications providers. We believe that reform is overdue, and the introduction of an IPB is timely.

BT submitted a detailed response to David Anderson QC's recent review of investigatory powers and will continue to seek to influence Government as the debate on investigatory powers gathers momentum. Our underlying position remains as set out in our response to that review:

"We consider that it is appropriate to maintain a regime that permits access to content and communications data, provided that the circumstances are suitably circumscribed, and provided that all necessary checks and balances are in place to ensure the lawful and proportionate operation of that regime, particularly from a human rights perspective."

We believe that the Government must have appropriate investigatory powers to protect society and balance the need to protect customers' privacy and rights. But those powers should also protect the rights established in the European Convention on Human Rights (as implemented in the UK by the Human Rights Act 1998) and the European Union's Charter of Fundamental Rights. Better oversight and transparency are crucial for the new regime. Strong law, with clear safeguards throughout the process, should give everyone confidence that intrusive powers will only be used when necessary. For BT, it is crucial that our customers can share that confidence. We comment in more detail on these issues later in this response.

BT's interests are not confined to the substantive powers and oversight provisions contained in the IPB. We believe that the new regime should also reflect the principles outlined below.

2. Level playing field

To ensure competitive fairness, we consider that it is imperative for the new regime to apply a level playing field for all communications service providers (CSPs) in the UK. The initial or primary obligation to assist, and to maintain a technical capability, should sit with the CSP with the closest relationship to the end user; that CSP will be best placed to be able to provide the required information (without needing to either filter out or provide other data, which would be the case if the request were made of a 'wholesale' network operator, rather than at the "retail" level).

We are therefore concerned that clause 189 of the IPB extends Government's power to serve a capability notice on a CSP to cover all the "telecommunications services" it provides, rather than just "*public* telecommunications services", as under the current regime. BT offers a significant range of services that do not fall into the "public" category. Examples

include services offered under compulsion (Wholesale Line Rental or Local Loop Unbundling offered by BT Openreach) and private networks (a network provided to a large company for internal communications). This change could have significant implications for BT.

Moreover, we do not think it is clear on the face of the Bill in what circumstances a CSP like BT might be required to retain or hand over data relating to services offered by third parties, for example, UK based CSPs or overseas based CSPs, like twitter and Facebook, amongst many others. In any event, we do not believe that Government has provided a compelling case that UK-based CSPs like BT should keep data relating to any other CSPs.

3. Cost recovery

The IPB makes provision for CSPs to receive an "appropriate contribution" of their relevant costs. We believe that the law should require full cost recovery for all CSPs. The capability provisions are very wide and the costs that CSPs are likely to incur will be significant. They will need to generate or obtain, retain and disclose data for which they have no business need, and since these obligations are necessary to protect society, we believe that these costs should be borne by the Government, not by CSPs, or their customers.

We should also flag that it is not possible for us to give a final estimate of the costs likely to be incurred without additional information about the capability required. However, depending on the assumptions made, the costs of a capability across industry over 10 years may be significantly more than the cost estimates we have seen to date from the Government. We also think that in in any event, attempting to predict costs over a 10-year period will be difficult, given the rapid technological changes the industry has seen in the previous 10 years; an estimate over a maximum of five years is more likely to be realistic.

4. CSPs should be compelled to assist

Subject to the right checks and balances being in place, we see a strong case for CSPs being compelled to provide help as law enforcement and security agencies seek to exercise their powers under the IPB. We recognise that the Bill removes some discretionary elements from the current regime. But others are still there, notably on disclosing communications data. We think that these should be removed.

5. Encryption

We want to comment on the issue of encryption in our response, as it is a good example of the challenges the Government faces in getting the new law right. Both David Anderson QC and the Government believe that there should be no "dark areas" in communications. Their worry is that if communications can't be decrypted, criminals and terrorists will be able to place themselves beyond the reach of the law, by using methods of communication which cannot be accessed or understood by public authorities. This is one side of the debate. On the other side, encryption helps people communicate securely. More and more people use the internet as part of their daily lives, for banking, shopping and storing or accessing personal information. Encryption gives people confidence as it reduces the potential for cybercrime. It empowers free expression in countries without a strong and independent legal regime.

Encryption is a difficult area, with complex technology. Sometimes there will be practical constraints on what a CSP can do, for example, if the data it carries has been encrypted by a third party, then that CSP simply may not be able to decrypt it.

The availability of a decryption key creates a weakness in the security of the encryption. It is for Parliament to debate whether or not the creation of such a weakness is justified for other reasons, for example crime prevention or national security.

The arguments on both sides of the debate are compelling. Close engagement between Government and industry will be key to finding a way forward.

Overarching questions

6. **Are the powers sought necessary?** ***Has the case been made, both for the new powers and for the restated and clarified existing powers?***

This is primarily an issue for Government to determine, although we note that some existing powers are also being challenged through the courts. However, we do not believe that to date a compelling case has been made to require communications providers to retain third-party data. We also believe that the proposals for retention on internet connection records require careful evaluation in terms of their proportionality, feasibility and cost.

7. **Are the powers sought legal?** ***Are the powers compatible with the Human Rights Act and the ECHR? Is the requirement that they be exercised only when necessity and proportionate fully addressed? Are they sufficiently clear and accessible on the face of the draft Bill?***

Whether or not the substantive powers sought, and the exercise of those powers, are legal is ultimately a matter for the courts to determine. As matters stand, there are a number of cases (some resolved, some pending) that may have an impact on the Government's proposals, some of which we referred to in our recent report, as below.

- The Data Retention Directive: in April 2014 the Court of Justice of the European Union (CJEU) declared this invalid in the Digital Rights Ireland case because it did not comply with the principle of proportionality. Its interference with the right to privacy was not limited to what was strictly necessary: *"although the retention of data required by the directive may be considered to be appropriate for attaining the objective pursued by it, the wide-ranging and particularly serious interference of the directive with the fundamental rights at issue is not sufficiently circumscribed to ensure that that interference is actually limited to what is strictly necessary."*

- Data Retention and Investigatory Powers Act (DRIPA): in July 2015, following a judicial review brought by David Davis MP and Tom Watson MP, the High Court held that parts of DRIPA were not compatible with Article 7 (respect for private and family life) and Article 8 (protection of personal data) of the European Union's Charter of Fundamental Rights. The Court held that access to communications data should be (a) limited to cases of serious crime or national security and (b) subject to

judicial/ independent approval. The Court of Appeal has subsequently suggested that neither requirement is necessary but has referred the case to the CJEU for further clarity on the decision in the Digital Rights Ireland case.

- Bulk interception: in September 2013 Big Brother Watch asked the European Court of Human Rights (ECtHR) to review whether the UK's surveillance laws were compatible with the European Convention on Human Rights. This claim was then put on hold because of a similar challenge at the Investigatory Powers Tribunal (IPT), brought by Liberty, Amnesty International and Privacy International.

  The IPT found in December 2014 that the UK's bulk interception regime did not contravene Convention rights. Liberty, Privacy International and Amnesty International effectively appealed this decision by filing a claim at the ECtHR in April 2015.

- Safe Harbor – in October 2015, the CJEU made an important decision on data protection in the Schrems case. It said that the Safe Harbor scheme (under which personal data can be transferred from the EU to registered bodies in the US) doesn't adequately protect data. One reason was that the scheme may not be able to stop the US intelligence authorities accessing the transferred data on a large scale, which is not compatible with the right to privacy in the EU Charter of Fundamental Rights.

- Equipment interference: Privacy International is currently challenging the Government's use of computer network exploitation in the IPT (see IPT 14/85/CH). The hearings have now commenced. Privacy International state they have also taken their case to the ECtHR.

It remains to be seen what impact these cases, and any further challenges- particularly in the context of retention of ICRs, might have on the substantive powers sought by Government.

The retention of ICRs represents the main new capability in the IPB. The precise requirements of the Bill in this context are difficult to follow. As we understand it, the Government wants CSPs to retain the domain names visited by users over a 12-month period. However, a list of these domain names could reveal sensitive personal data about an individual, for example, information about their medical condition or sexual preferences. The Digital Rights Ireland case suggests the existing retention obligations under DRIPA may be close to the boundary of what is lawful under EU law. The additional requirement to retain ICRs could lead to fresh challenges on human rights grounds.

It is a point of potential concern that we may have to implement certain capabilities, and to incur costs, before a number of legal issues we have referred to are resolved, but we also recognise that it is not practicable for the Government to delay introduction of the Bill until all these are settled.

As for necessity and proportionality, these are difficult yardsticks to assess. It is one thing for the Bill to expressly require that the various powers are used only when necessary and

proportionate, but quite another to be able to demonstrate that these requirements have been met. Better oversight and transparency is crucial. Strong law, with clear checks and balances in place from the start of the process (authorisation) to the end (audit), should give everyone confidence that intrusive powers will only be used when necessary and that any interference with the right to privacy will be kept to a minimum. Regular review of the operation of the law, with input from stakeholders, is important to keep pace with change.

We welcome the proposed creation of the Investigatory Powers Commissioner (IPC) to provide independent oversight, with an expanded remit and greater resources. It should have full powers to disclose an accurate and complete picture of the total number of requests made which affect individuals. In addition, if CSPs have concerns about the necessity or proportionality of what they are required to do, they must be able to have confidence that the IPC has the requisite authority and resource to review matters, and to make appropriate decisions. We comment further on the proposed authorisation regime later in this response.

As for the clarity and accessibility of the powers on the face of the IPB, we have not yet completed our detailed analysis of the draft and so cannot give a full answer. The IPB is long and technically complex, and we have noted to date that there are a number of points of potential confusion. For example, there appear to be two separate definitions of ICRs; and the assessment of proportionality that the IPC may be required to make appears to be different, depending on whether it is considering whether to authorise a warrant or an appeal from a CSP.

8. ***Is the legal framework such that CSPs (especially those based abroad) will be persuaded to comply?***

The legal framework is mandatory for CSPs in the UK so they must comply. It is difficult for us to comment on whether overseas CSPs will comply. The introduction of judicial authorisation may persuade some overseas CSPs of the legitimacy of requests for interception.

As we understand it, CSPs based overseas but offering services in the UK may be asked to disclose information in the UK. But such a request could conflict with their own country's laws and provide grounds for refusal, depending on where their operations are located. Furthermore, retention notices are not binding on overseas CSPs.

If overseas CSPs are concerned about the jurisdictional reach and scope of the draft Bill, and, as a result, are less minded to co-operate with a request, then that could have a clear impact for UK-based CSPs, in terms of being asked to assist with increased numbers of third party-data requests.

We agree with the recommendations from the published summary of the Sheinwald Report which looked at this area in detail. There should be better co-operation between like-minded Governments in different countries for the efficient exchange of information necessary to prevent terrorism, detect crime or to deal with risk-to-life situations. The mutual legal assistance treaty (MLAT) process should be improved to allow Governments to

obtain information directly from CSPs in different jurisdictions, in accordance with their local laws, with more transparency and co-operation between requesting authorities and local companies.

9. ***Are concerns around accessing journalists', legally privileged and MPs' communications sufficiently addressed?***

We have no comment here.

10. ***Are the powers sought workable and carefully defined? Are the technological definitions accurate and meaningful (e.g. content vs communications data, internet connection records etc.)? Does the draft Bill adequately explain the types of activity that could be undertaken under these powers? Is the wording of the powers sustainable in the light of rapidly evolving technologies and user behaviours? Overall is the Bill future-proofed as it stands?***

We agree that the draft Bill needs to be proofed against future technological change, but this is a very complex issue. Any new legal definitions must balance the need to cover a broad range of factual circumstances with providing legal certainty. They must also ensure that the most intrusive types of data attract the strongest legal protection before they can be accessed.

We find some of the proposed definitions complex and difficult to follow, particularly the definition of content. Content is defined as that: "which reveals anything of what might reasonably be expected to be the meaning of the communication." This is a non-technical, subjective description (and it might perhaps be better described as the "substance" of a communication). We do not see that it has much resonance in the context of a telephone communication, where the content is the conversation, and it does not really clarify the position in relation to URLs.

The carve-outs from the definition of content are also unclear (for example, for meaning arising from the "fact of the communication" or, in relation to web browsing, for anything "identifying the relevant telecommunications service").

The Explanatory Notes accompanying the Bill state that domain names (for example, bbc.co.uk) are communications data but a URL is content (para 451). We have some difficulty accepting the conclusion that URLs are content from the drafting:

- does the file path in the url reveal the "meaning of the communication", ie, is it content in the first place? This is not clear. Presumably it would be in the case of a Google search as it reveals details of a query. What about a dynamically created URL? Does it depend on the URL in question?
- Content does not include anything that identifies the telecommunication service in question. What does this mean? What if the URL identifies the service used (for example, a feedback form)? Does that mean it ceases to be content? Of is the "telecommunication service" the website as a whole?

- Content does not include any meaning arising from any data relating to the transmission of the communication. Does the URL relate to the transmission of the communication? It is hard to see how the relevant web page could be returned without the URL.

The term "telecommunications service" also appears to be unclear, when considered in the light of the Explanatory Notes. It is defined as "any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service)". The Explanatory Notes suggest that a telecommunication service includes a website such as bbc.co.uk. However, it is difficult to see how the definition leads to this conclusion. This is not what one would ordinarily think of as a "telecommunications service", unlike say Hotmail or Skype.

We recognise that the distinction between communications data and content is a very important issue but are not convinced that seeking to define both exhaustively is the right approach (especially in the absence of a catch-all provision for data which does not fall easily into either category). Our suggestion for an alternative approach would be:

- Provide a simple definition of communications data and treat everything else as content, with examples in secondary legislation as to what data sets are entity data and what are events data;
- The Secretary of State should have the power to issue Regulations for a particular type of communication (e.g. web browsing) that set out exactly what is content and what is communications (entity/ events) data. This would help with legal certainty and transparency, but would also provide the necessary flexibility for certain data sets to be upgraded, if appropriate;
- For example, for telephone calls/SMS, subscriber information could be designated as entity data and signalling information as events data (time, location, caller number, recipient number, duration etc). By default, the conversation would be treated as content;
- For internet use, the information in an IP packet header (source IP, destination IP, date, length, type of service etc) could be designated as communications data, with the payload of the packet (by default) as content; and
- The IPC should have the power to request the Secretary of State to issue Regulations in cases where there is uncertainty.

One further point concerns the practical implications of any third-party data request, for example a targeted "obtain and disclose" request made to BT to obtain communications data in relation to the use of a Facebook service. If such a request were made directly to Facebook, then it would be easily able to locate and provide only the required communications data. If, alternatively, such a request were made to BT, BT would need to comply with that request in a more privacy intrusive manner because we would need to examine all the data, including content, to work out which particular communications data was relevant to the request.

11. Are the powers sought sufficiently supervised? Is the authorisation process appropriate? Will the oversight bodies be able adequately to scrutinise their

operation? What ability will Parliament and the public have to check and raise concerns about the use of these powers?

As we stated in the introduction, all the powers in the IPB should protect the rights established in the European Convention on Human Rights (as implemented in the UK by the Human Rights Act 1998) and the European Union's Charter of Fundamental Rights. Bulk powers on interception, communications data and equipment interference, which are potentially extremely privacy–intrusive, should only be used in very rare circumstances, when all other capabilities have been considered.

We believe that judicial authorisation is needed for these more privacy-intrusive powers and therefore support the proposal to mandate this for all warranted activity. We also believe that there is a case for extending judicial authorisation to data retention notices and national security notices, but support the proposal to give CSPs a direct right of review to the Secretary of State (SoS) in both cases (with the SoS having to take into account the IPC's views on proportionality).

We believe that there is a case for extending the review mechanism to bulk warrants. CSPs have no ability to challenge any obligation to assist with equipment interference, bulk interception or bulk equipment interference, nor to be consulted prior to their issue. Whilst CSPs are not required to take steps that are not "reasonably practicable", the assistance sought under these powers is likely to be bespoke and could be controversial.

For example, assistance with equipment interference might damage the security of the CSPs systems or might conflict with other legal obligations on the CSPs to secure their networks. We think there should be a formal right for CSPs to challenge these powers. In any event, CSPs should have a general right to report matters of concern to the IPC, and the IPC should be under a general power to investigate those concerns.

In all cases where a Judicial Commissioner is required to make an assessment of proportionality, he or should be empowered to do so on the merits of the case: the assessment should not be limited to procedural matters. We believe that this will help to build public confidence in the authorisation and oversight regime.

Whether or not the oversight bodies will be able to provide an appropriate level of scrutiny, and the extent of Parliamentary and public confidence in that scrutiny, will depend on a range of factors, including the:

- volume of warrant applications/ appeals and degree of urgency required
- resource and expertise available to the IPC
- extent to which the IPC has understanding of broader security context (eg overall level of threat). There is a case for introducing some sort of process to appraise and update the Judicial Commissioners of these issues
- extent to which CSPs are able to refer matters of general concern to the IPB
- powers available to IPC to investigate those matters referred.

General questions

12. To what extent is it necessary for (a) the security and intelligence services and (b) law enforcement to have access to investigatory powers such as those contained in the Draft Investigatory Powers Bill?

Please refer to our comments in the Introduction section. We believe that it is appropriate for Government to have access to investigatory powers, subject to there being suitable safeguards in place.

13. Are there any additional investigatory powers that security and intelligence services or law enforcement agencies should have which are not included in the draft Bill?

We have no comments here.

14. Are the new offences proposed in the draft Bill necessary? Are the suggested punishments appropriate?

We believe there should be proper sanctions to ensure the rules in the draft Bill are enforced. For this reason we support the new offence of unlawfully obtaining communications data, albeit it is drawn in narrow terms.

The IPB continues the restriction on disclosing information about interception activities. It also contains new restrictions on revealing information about the disclosure of communications data or the imposition of a retention notice.

However, these restrictions are implemented in slightly different ways. For example:

- the secrecy provisions for interception allow disclosure to legal advisers;
- a person served with a national security notice or technical capability notice cannot disclose its existence or contents to any other person;
- the provisions relating to the acquisition of communications data prevent disclosure without "reasonable excuse" but do not expressly permit disclosure to legal advisers; and
- the provisions relating to retention notices do not make disclosure of the notice an offence and instead simply place a duty on CSPs not to disclose.

The Government should take a consistent approach to these provisions. With such wide ranging restrictions, it is all the more important that the IPC is able to provide as much transparency as possible in its reports about how each power is used.

Interception

15. Are there sufficient operational justifications for undertaking (a) targeted and (b) bulk interception?

Whilst we are able to provide information on technical feasibility/ degree of difficulty and the cost implications of these- and other – capabilities, it is primarily a matter for Government to determine whether there are sufficient justifications.

However, we acknowledge that bulk interception is controversial. A UK court has said that the current rules are lawful and comply with human rights. David Anderson QC believes that Government has shown it needs these powers for both content and communications data- but some privacy campaigners believe that bulk interception is too great an infringement of privacy in a free society.

Our view is that Government should be able to use bulk powers provided the pending legal cases uphold their validity, and that strong oversight means that they are only used when it is necessary and proportionate to do so. This essentially represents our view on all relevant powers: provided that they are lawful in principle, and there are appropriate safeguards in practice, we think it is legitimate for Government to exercise them.

In this specific case, however, we consider that some further explanation of what is meant by "bulk", either on the face of the IPB or in guidance material, would enable greater transparency and so assist for the purposes of determining proportionality.

16. Are the proposed authorisation processes for such interception activities appropriate? Is the proposed process for authorising urgent warrants workable?

Please refer to our earlier comments on the authorisation process.

The approach to authorising urgent warrants appears to be appropriate. Section 20 applies where an urgent warrant is issued without approval of a Judicial Commissioner. It requires the person who issued the warrant to inform a Judicial Commissioner who must review it unless it is formally renewed (which also requires approval of Judicial Commissioner). This appears to provide sufficient oversight. For example, if the Judicial Commissioner were to believe that urgent warrants were being repeatedly issued to circumvent the approvals process, they could simply inform the IPC.

17. Are the proposed safeguards sufficient for the secure retention of material obtained from interception?

This is primarily a question for a requesting authority to answer.

18. How well does the current process under Mutual Legal Assistance Treaties (MLATs) work for the acquisition of communications data? What will be the effect of the extra-territorial application of the provisions on communications data in the draft Bill?

Please refer to our earlier comments on MLATs.

Communications Data (Acquisition)

19. Are the definitions of content and communications data (including the distinction between 'entities' and 'events') sufficiently clear and practical for the purposes of accessing such data?

Please see our earlier comments about the difficulties with some of the new definitions.

The distinction between 'entities' and 'events' appears sensible, but of limited application. Its primary function is to determine the minimum office, rank or position needed to acquire the relevant data in Schedule 4. Events data is considered to be potentially more intrusive and therefore requires a higher level of authority for acquisition.

20. Does the draft Bill allow the appropriate organisations, and people within those organisations, access to communications data?

We have no comments here. This is an operational issue.

21. Are there sufficient operational justifications for accessing communications data in bulk?

We have no comments here. This is an operational issue.

22. Is the authorisation process for accessing communications data appropriate?

As we said earlier, the CJEU is considering whether access to communications data ought to be: (a) limited to cases of serious crime or national security; and (b) subject to judicial approval (although we would question how judicial approval would work given that there are hundreds of thousands of requests made each year).

Data retention

23. Do the proposed authorisation regime and safeguards for bulk data retention meet the requirements set out in the CJEU Digital Rights Ireland and the Court of Appeal Davis judgments?

See our earlier comments, the CJEU is considering this question.

We think the issue of a data retention notice should be subject to the approval of the Judicial Commissioners, though we note a CSP has the power to challenge a retention notice by referring it to the Secretary of State. It is not clear what standard of review the Secretary of State would apply.

24. Is accessing Internet Connection Records essential for the purposes of IP resolution and identifying of persons of interest? Are there alternative mechanisms? Are the proposed safeguards on accessing Internet Connection Records data appropriate?

It is helpful to provide some background information about ICRs before answering this question.

ICRs do not currently exist and we [CSPs] do not need them in order to attribute IP addresses to users or for normal business purposes. So, this proposed requirement would mean that CSPs would have to generate and retain data that they currently do not, which represents a significant new development.

The consequences for CSPs of being required to generate ICRs could be significant. For example, a CSP might have to change how its service is provided. For BT WiFi, we offer a free 'click and connect' service that does not require user details to be provided or verified. To comply with any obligation to generate ICRs, we -and other CSPs may have to offer only authenticated, registered access.

We understand that the intention is to require CSPs to retain (under a data retention notice) for up to 12 months, a record of sites visited and online applications and services used. This data can then be queried for specified purposes when appropriately authorised.

We need clear information from Government about what CSPs may be required to generate and retain and when, for example under a data retention notice, or as part of a forward-looking targeted acquisition request. For additional clarify, it would be helpful if Government would explain how the new types of data which fall within the ICR provisions are different from those that fall within the current regime. This will allow CSPs properly to scope capability and cost, and to identify what methods we could employ to generate ICRs.

The collection of ICRs could be complex and costly in practice. For example, if an individual visits a particular website, they could generate multiple ICRs, as the website may be composed using content drawn from multiple locations across the internet. This content may include adverts, social media plug-ins, review plug-ins, news feeds, etc. Where cookies and other website tracking technologies are used, this content may be compiled dynamically and be related to the historical activities of more than one user of a device.

It is therefore difficult to separate ICRs which relate solely to a "communications service", and this might lead to retention and disclosure of information beyond that which is required. Further work is required to determine how to limit the volume of data disclosed. CSPs should not be required to manage and implement data filtering.

Increased use of encryption means it will be more difficult in the future to extract meaningful data to match the purposes for which it is to be retained.

The safeguards on accessing retained data (namely that it can be used only for the three specific purposes and not accessed by local authorities) appear sensible, given the potential intrusiveness of ICRs (but please refer to our earlier comments about the possibility of a legal challenge).

However, as we understand it, the IPB does not treat all ICRs in the same way, and these safeguards do not apply in all cases. For example, ICRs have different meanings in the retention and access provisions (clauses 71 and 47). For example, CSPs must retain an "internet protocol address, or other identifier". But, the additional protection against

disclosure only applies to data that is used to identify a "telecommunications service". Much depends on the definition of "telecommunications service" which is currently unclear.

Also, the three restrictions on use apply to retained data, but not to either targeted "obtain and disclose" acquisition requests or bulk acquisition powers.

The Government should clarify if these differences are intentional and should explain the reasons for them.

25. Are the requirements placed on service providers necessary and feasible?

The answer depends on the exact requirements to be placed on CSPs, and we do not have full information yet about that. We have the following concerns at this stage:

- a retention notice could require us to not only retain but also process or generate communications data that we would not otherwise do
- an obligation to generate and retain ICRs would be new and onerous
- The obligation to retain data, potentially includes not only communications data from our customers but also communications data for third party communications we carry over our network (see section 46(5)(c)). We would be very concerned about the practicalities of doing this and the proportionality of doing so
- security of this communications data is very important, especially with the growing threat from cyber-crime and hacking. The loss or disclosure of ICRs would be extremely serious given the potentially intrusive nature of the information it would reveal about individuals
- retention notices should only be served on CSPs providing public telecommunication services and networks, as is the case under the current regime. As we explain in our opening comments, there should be a level playing field for all CSPs. The obligation should fall on the operator with the closest relationship to the end user as that provider is most likely to have access to the information in question.

Equipment interference

26. Should the security and intelligence services have access to powers to undertake (a) targeted and (b) bulk equipment interference? Should law enforcement also have access to such powers?

We understand that the growing use of encryption and the range of communication technologies (e.g. Twitter, WhatsApp, iMessage) mean that it is increasingly difficult to access communications via traditional interception methods. We understand why Government considers it needs these powers.

As we commented earlier, our view on all relevant powers is that provided that they are lawful in principle, and there are appropriate safeguards in practice, we think it is legitimate for Government to exercise them. Bulk equipment interference is arguably the most potentially intrusive of the powers, and the threshold for establishing proportionality and necessity should accordingly be very high.

27. Are the authorisation processes for such equipment interference activities appropriate?

This is an intrusive power. It should be approved by both the Secretary of State and the Judicial Commissioners.

28. Are the safeguards for such activities sufficient?

Please refer to our earlier comments. We think CSPs should have a right of appeal against the imposition of obligations in respect of these powers. The Bill should also state expressly that it is not reasonably practicable for CSPs to provide assistance if they reasonably believe that assistance would compromise the security of their network. In particular, if CSPs were to compromise their network that would conflict with their security obligations under Privacy and Electronic Communications Directive and the Framework Directive, neither of which contain an exemption for national security or crime prevention purposes.

Bulk Personal Data

29. Is the use of bulk personal datasets by the security and intelligence services appropriate? Are the safeguards sufficient for the retention and access of potentially highly sensitive data?

We have no comments here.

Oversight

30. What are the advantages and disadvantages of the proposed creation of a single Judicial Commission to oversee the use of investigatory powers?

We welcome the appointment of the IPC as a 'super' regulator, with greater resources and remit, to deliver effective scrutiny of the use of the powers. It is helpful that the Prime Minister can direct the IPC to oversee new areas, to keep pace with developments within the security and intelligence agencies.

The draft Bill should make clear when the IPC has the lead rather that the Information Commissioner, for example in relation to security of data requirements and breach notification. These are two areas where the regulatory regimes overlap, but there should not be any confusion about reporting requirements. It is helpful that IOCCO and the ICO are in active discussions to agree a memorandum of understanding for CSPs. We suggest that IPC will be the most competent regulator for national security considerations arising out of personal data security breaches and for ensuring that data retained or disclosed is processed with tight security measures to prevent unauthorised access.

31. Would the proposed Judicial Commissioner have sufficient powers, resources and independence to perform its role satisfactorily?

Please see our earlier comments about whether a judicial commissioner will have the time or full knowledge to review all requests.

It would be helpful overall if the IPC, as part of his annual reporting, were to provide as much information as possible about the use the powers under the draft Bill. This is particularly the case where the powers do not exactly match up to those under RIPA. For example, the draft Bill allows an interception warrant to be used for an "operation". This could be used to intercept the communications or tens or even hundreds of people but this would not be obvious from fact a single warrant had been issued.

32. Are the appointment and accountability arrangements for Judicial Commissioners appropriate?

We have no comments here.

33. Are the new arrangements for the Investigatory Powers Tribunal including the possibility of appeal adequate or are further changes necessary?

We support the right to appeal a decision of the IPT.

In closing, we refer the Committee to our written submission (Annex 1) to the Science and Technology Committee, of November 2015, which sets out our comments on the questions considered by that Committee. Mark Hughes, president, BT Security, gave oral evidence to the Science and Technology Committee on 8 December 2015, and to the Joint Committee, as part of a panel of CSPs on 9 December 2015.

We would also like to refer the Committee to BT's report on privacy and free expression in UK communications, published on 10 December 2015. That report, which includes our observations on the current investigatory powers regime and our initial thoughts on the proposed new one, is available here.

Annex 1

The Science and Technology Committee Inquiry Investigatory Powers Bill: technology issues

Evidence from BT
November 2015

Submission to the Science & Technology Select Committee Inquiry

Investigatory Powers Bill: technology issues

Introduction

BT welcomes the Science and Technology Select Committee's Inquiry into the technology issues arising from the draft Investigatory Powers Bill (IPB).

Publication of the IPB means that, for the first time, there is one document that sets out the totality of investigatory powers that government considers necessary in relation to communications providers. We believe that reform is overdue, and the introduction of an IPB is timely.

BT submitted a detailed response to David Anderson QC's recent review of investigatory powers and will continue to seek to influence government as the debate on investigatory powers gathers momentum. We are currently undertaking a detailed analysis of the Bill and hope to complete this shortly. Our intention is to provide a comprehensive written response by 21st December to the Joint Committee on the Investigatory Powers Bill.

However, our underlying position remains as we set out in our response to the Anderson Review:

"We consider that it is appropriate to maintain a regime that permits access to content and communications data, provided that the circumstances are suitably circumscribed, and provided that all necessary checks and balances are in place to ensure the lawful and proportionate operation of that regime, particularly from a human rights perspective."

We believe that the government must have appropriate investigatory powers to protect society and balance the need to protect customers' privacy and rights. But those powers should also protect the rights established in the European Convention on Human Rights (as implemented in the UK by the Human Rights Act 1998) and the European Union's Charter of Fundamental Rights. Better oversight and transparency are crucial for the new regime. Strong law, with clear safeguards throughout the process, should give everyone confidence that intrusive powers will only be used when necessary. For BT, it is crucial that our customers can share that confidence.

BT's interests are not confined to the substantive powers and oversight provisions contained in the IPB. To ensure competitive fairness, we consider that it is imperative for the new regime to apply a level playing field for all providers of communications services in the UK. And we believe that it should be made expressly clear that all eligible costs incurred by those providers should be met by government.

Our initial views on the specific matters raised by the Committee are set out below.

<u>The technical feasibility and costs of meeting the obligations imposed by the Bill</u>

We are still considering the technical feasibility and costs associated with meeting the obligations of the IPB. Many of the powers contained in the Bill (eg, lawful interception and obtaining of communications data) are derived from those already contained in RIPA and other associated legislation. These are well understood and should not pose difficulties from a technical perspective. However, it is difficult to provide an estimate of likely cost even where we are familiar with the technical capabilities, given that we cannot predict the level of technical capability that we may be required to maintain under the new regime; the level

of subsequent deployment of each capability; and, in the case of data retention, the scope of any retention notice that may be imposed on BT.

The position on technical feasibility and cost is even harder to assess in the light of new powers, and corresponding capabilities, envisaged in the IPB. The most significant of these is the proposed requirement to retain "internet connection records" (ICRs). We understand the intention here in broad terms is to require internet service providers to retain (under data retention notices) a record of sites visited/online applications and services used. The Home Secretary has compared them to itemised call records.

Whilst the concept of an ICR may seem relatively straightforward, the introduction of a capability to retain them will be less so. Leaving aside issues relating to the definitions of ICR contained in the Bill (there are two), BT does not currently generate (or retain) a single set of data that is capable of meeting the proposed requirement. We are currently scoping what data sources and methods we could employ to generate ICRs.

There is a range of options available. As matters stand, we believe that the most cost-effective approach may be one that at least partly relies on sampled network flow records that are currently available for business purposes. However, as the description implies, not all relevant IP flows would be retained, and so it is likely that some ICRs may not be captured. We would be happy to provide further technical detail to the Committee on this and other possible solutions.

However, in order to progress the issue, we require greater clarity as to what we may be required to generate and retain in what circumstances (ie, retention under a data retention notice versus targeted acquisition); and, primarily in the context of a retention notice, some indication of the likely scope of any obligation that government may impose. Without this information, we cannot realistically scope technical feasibility or cost. And against this backdrop, we are not clear on what basis government has decided to set aside £175m towards the costs of retaining ICRs.

<u>The impact on communications service providers and related businesses</u>

The implementation of the measures proposed within the IPB introduces areas that need close scrutiny and consideration by communications service providers (CSPs) and others falling within the scope of the Bill. As described above, we are able to scope the technical feasibility of some elements of the IPB relatively easily, but some are new. On overall cost, again as indicated above, we are not yet able to give a meaningful estimate. Whilst we believe it is extremely helpful for all relevant substantive powers to be included in a single statute, we are not yet clear as to the extent to which they may be applied in practice. We also note that the IPB envisages that arrangements must be in place for telecommunications operators to receive an "*appropriate contribution*" to their relevant costs. This creates further uncertainty. We believe that all our eligible costs should be met, especially since we may be generating and retaining, to rigorous security standards, data for which there is no business need.

<u>The likely consequences for citizen/consumer use of ICT services</u>

Again, it is too early to predict accurately the possible consequences for citizens and consumers. However, at this stage we do not anticipate that the IPB will have a major impact on their use of ICT services, provided that both government and industry are as transparent as they reasonably can be on the nature of the powers available, and the new oversight body provides as much information as it can on the subsequent implementation of those powers. It will be important too to be able to demonstrate that the new regime applies equally to all communications service providers operating in the UK.

It is nevertheless likely that certain issues addressed by the Bill will have greater resonance with citizens and consumers than others. For example, the importance of encryption in securing the privacy of customer communications, and the extent to which government should be able to access the content of those communications, are issues that are already a matter for public debate. Similarly, there is currently significant interest in the measures service providers take to protect their customers' data. This may well increase if it is perceived that we may be required to retain more of that data (such as ICRs). We will of course continue to take a close interest in these and other related matters.

6 January 2015

Kevin Cahill—written evidence (IPB0145)

Status (locus) for giving this evidence.

I practice as a journalist and author but am, by profession, a systems analyst and a specialist in the use of supercomputers, the machines that will mainly be used to implement the provisions of this Bill, if enacted.

Recently I have litigated before the County Court at Guildhall, London, and before the Investigatory Powers Tribunal, seeking to enforce privacy rights under HRA 8, and to end the criminal interception of my own emails and those of a number of children under DRIPA.

I have read all 300 pages of this Bill, line by line.

The Bill.

The Bill purports to make the process of investigating crimes such as terrorism, paedophilia and serious criminality easier, mainly for the 3 intelligence services, GCHQ, M16 and M15, but for other government agencies too.

The Bill seeks to achieve this aim by severely limiting and restricting the rights of UK citizens to their privacy rights under the HRA 8.

The Bill is 300 pages long . The HRA is 26 pages long. The Privacy provision in the HRA occupies one page of that statute.

The predecessor act, RIPA, then DRIPA, were judged unfit for purpose by Mr David Anderson QC, the advisor on anti terrorism legislation, the Intelligence and Security Committee of Parliament and by a specially prepared report of the Royal United Services Institution.

The preceding act, DRIPA was ruled incompatible with the privacy provisions of the HRA by the High Court on 17/7/2015

HMG appealed the verdict and lost. The Appeal Court has referred the High Court judgement to the European Court of Justice 24/11/2015

At even its simplest reading this Bill, not merely limits privacy, but seeks to abolish the concept altogether for some citizens of the UK. It is likely therefore to be found incompatible with the HRA. HMG's approach to this is to abolish the HRA , thus de linking the ECHR from its English common law roots in the right to security of a domestic dwelling that preceded Magn Carta, and is expressed in the ancient cliché that ' an Englishman's home is his castle'. In this Bill HMG seeks to give itself spying powers in the home that only the Nazi and Stasi regimes in Germany and in East Germany possessed or tried to possess.

Is the Bill a hybrid Bill ? Hybrid Bills are those which mix public and private matters.

The Bill gives HMG the power to do what HMG calls 'Bulk Collection'. This is a semantic legalism designed to conceal the fact that 'Bulk Collection' is 'Mass Surveillances' but only of some people in the UK, those who use the Internet.

According to UN statistics for 2014, reproduced in Internet Live stats, the population of the UK is 63,489,234 persons. According to the same figures 57,075,825 person in the UK use the Internet. This leaves 6,413,409 persons who will not have their data 'Bulk Collected'.

This legal and constitutional distortion, dividing the UK population into those who use the Internet and those who don't, alone points to a serious constitutional flaw in this bill. But it points to an equally serious operational one for the services that the Bill is supposed to be there to assist. The exclusion of such a large element of the population from the provisions of the Bill, and the creation of what amounts to a 'safe haven' from Government surveillance, points the way forward for the intelligent terrorist; off the internet into the unsupervised area. The incentives are high to do that given recent successes in killing terrorists in the Middle East, using technological means. The only terrorist suspects who will use the web now will be those ignorant of its scope and capability for use in detecting their activities. This is not Snowden. This is this Bill.

There is a further operational hazard created for the Intelligence Services by the approach to surveillance used in the Bill. The number of terrorists loose in the UK and accessible to UK technology at any time, is very small, perhaps a maximum of 0.01% of the population ? This is often referred to as the 'needle' in the haystack issue. What 'Bulk Collection' does is point the would be terrorist to a safe haven, the unsupervised portion of Internet, thus clearing the haystacks of all but a few 'needles' mostly those who are ignorant or uninformed.

It can be safely assumed that the staff of the three intelligence services are amongst the brightest and best investigators we have, or indeed any nation has.

But what the bill does is flush the 'needles' out of the haystacks, while attempting to make the haystacks available for searching almost innumerable. This is needle searching by seizing all the haystacks in the whole country, shaking them out, and then deploying the best resources we have to search a universe of empty haystacks, emptied mainly by this Bill.

The private element of the Bill. The private beneficiaries of Bulk Collection.

HMG propose that the major internet companies, all of them private companies, most of them based in the US with prior loyalties elsewhere , will hold the 'Bulk Collection' for a year. On the 6th of October 2015 the European Court of Justice, following findings of fact by the High Court in Dublin, struck down 'Safe Haven', the agreement under which private data collected by the US internet companies was transferred to America.

The major findings of fact, by the Dublin Court and incorporated into the final judgement of the ECJ, were two. The first was that the US was engaged in 'indiscriminate mass surveillance' using the PRISM programme. The second was that the evidence of Edward Snowden, published in the Guardian and elsewhere in June 2013, was valid evidence and was so incorporated by the Court in its judgement.

About 67% of UK users of the Internet, about 38 million people, use the services of 9 internet companies identified in the ECJ evidence as PRISM corporations, which have been intercepting their clients data in the UK for about 7 years, and stealing their clients data for money for the same period, on behalf of the National Security Agency, a foreign intelligence agency with no legal standing in the UK. Intercepting communications in the UK without a warrant is a criminal offence, as the former Interception Commissioner Sir Anthony May

told the Prime Minister in his report on the 8th of April 2014. Sir Anthony May also pointed out that the theft of data on a scale equivalent to the PRISM 'take', would be unlawful.

Thus HMG proposes to store the 'Bulk Collected' data with private companies, many of them the major interceptors of data and thieves of data in the UK over the past 7 years. HMG proposes to advantage those companies by paying for this service, against which HMG has no assurances against the misuses of PRISM, which was contrary to the Five Eyes Agreement of 1947, but happened anyhow.

Bulk Collection of data. The abolition of privacy in the UK.

Put in terms those of my generation will understand, 'Bulk Collection' of data involves the recording by the Government of every letter you write, the date, time and location of posting, the name and details of the person it is posted to and also the contents of the letter. Alongside that information all the phone calls you make will be collected and filed, as well as any other data you put on the Internet or web. This is a wholly novel extension of Government power, is in complete contradiction to HRA 8 and other parts of the Act as well as to English common law concepts of personal rights.

However, it is also something else. Bulk data collection. The creation of a general warrant.

It is the creation of what amounts to a pre emptive general warrant, applied without grounds, to that portion of the population using the Internet, but not to that portion of the population not using the Internet. This abolishes the absolutely essential notion of innocence until proven guilty, and the notion of reasonable suspicion before a warrant is issued. The companies who will store this data are currently un convicted criminals in terms of UK law. There is no guarantee whatsoever that they will not supply this data to their home government, if so ordered. That is what they have done for the last 7 years, in spite of UK law.

Further technology itself is insufficiently developed for any creators of such databases to be able to give an absolute guarantee that they will not be broken into.

There is a further, extraordinary defect in the Bill.

It purports to be a measure to ensure that the privacy of the citizen survives while the Government goes about the business of protecting the state from criminal and unlawful intrusion, something it has signally failed to do for the last 7 years in relation to PRISM. The Bill at no point states the HRA 8 privacy right, and fails to relate the circumscriptions put forward, to the actual 'right'.

At no point in the Bill is there reasonable provision for an ordinary citizen to enforce, in a local court, at reasonable cost, any of the Bill's provisions.

Instead, the citizen is offered the Investigatory Powers Tribunal, a High Court forum, utterly unsuitable for the person most affected by this Bill, the ordinary citizen, to approach. I know because I did so on 10th December 2015. A good deal of the hearing dealt with why I had not used Judicial Review at the actual High Court. Like over 90% of the UK I do not possess the £10,000 to £20,000 it would have cost to go to the High Court, in an attempt to enforce a basic right. Between the 300 pages of the Bill and the cost, a basic right has been rendered

completely inaccessible, to its basic holder, the ordinary citizen. The law is here abused for the purpose of denying any citizen the right to reasonable redress against abuse or enforcement of a basic right.

The legal cliché says that ignorance is no defence in law. A Bill such as this one is, on any reasonable basis, utterly incomprehensible to the ordinary lay person, whose basic rights are rendered inaccessible by the unending, torturous legalese of the Bill's language. A day will soon come, and the sooner the better, when any lay person can say; if I cannot understand a law, I cannot and will not obey it. Nor should I have to. Further, if it costs hundreds of thousands of pounds to enforce my basic rights, what rights do I actually have ?

I approached the IPT because for 2 and a half years, since June 2013, HMG has had prima facie evidence of criminal and unlawful activity in the UK by the PRISM companies. No police force nor the Information Commissioner has either investigated that evidence or brought a prosecution. Since the 6th of October the PRISM companies have been, de jure if not de facto, convicted by the ECJ of being part of a wholly unlawful activity in the UK, PRISM. HMG remains in denial about the ECJ ruling and in denial about the use of PRISM in the UK.

This Bill affects about 3.5 million children between the ages of 3 and 17 who use the Internet. No provision has been made for this fact.

There was no lower age limit in the PRISM instructions issued by the NSA and sanctioned by the FISA court. There are about 3.5 million children between the ages of 3 and 17 using the internet at any time in the UK. There is no lower age for Bulk Collection in the Bill

This Bill purports to apply the general warrant, bulk collection, to children too.

Extraterritoriality.

The US has sought, since the end of World War 11, to extend its laws to the rest of the world.

PRISM was the most extravagant such exercise, prompted by the dominance of the internet by American companies. But PRISM in the UK, which is where it affected 38 million people, including 3.5 million children, also demonstrates the utter stupidity of imagining that one nation can impose its laws in other nations. PRISM could never be rendered legal in the UK without Parliamentary consent. This was never given and could not be given.

The attempt to assign extraterritorial jurisdiction to HMG in the Bill is the act of latter day Canutes. And a demonstration that HMG has learned nothing from allowing 38 million of its citizens to be subject to a foreign law that attempts to impose criminality in the UK.

From Kevin Cahill. Fellow of the British Computer Society. Supercomputer correspondent for Computer Weekly. Fellow of the Royal Historical Society (and FRSA, FRGS) BA

23 December 2015

Kevin Cahill—Further written evidence (IPB0162)

Investigatory Powers Bill. Evidence of the PRISM corporations, Microsoft, Apple, Facebook, Google and Yahoo.

Last week these corporations asked you not to put extraterritorial provisions in the Bill. They did not explain that, as a result of the extraterritorial provisions in the US Foreign Intelligence Surveillance Act (FISA), they have each been intercepting emails and stealing data in the UK since 2007.

The Interception Commissioner, the Rt Hon Sir Anthony May QC,PC, advised the Prime Minister in his report on 8th April 2014 that interception of e mails without a warrant in the UK is a criminal offence under DRIPA (RIPA) and the theft of data on this scale was unlawful in the UK under HRA(8).

These 5 companies, together with Skype and Hotmail, were indicted (and convicted) for both those offences in Europe and the UK, by the European Court of Justice on the 6th of October 2015. None of these companies made application to be heard in the ECJ process, which was open to them. To have denied the facts in the case against them would have involved perjury.

The legal onus of applying the ECJ ruling has fallen to the UK Information Commissioner, Christopher Graham, a witness to you, who has done nothing to carry out his statutory duties so far. The legal duty of investigating the criminal interception falls to the police, who have done nothing either. You might raise this with the Home Secretary on the 13th, the Investigatory Powers Tribunal on the 10th of December 2015 having notified two police forces, the Met and the Devon and Cornwall Police, of sworn evidence in the matter, including that of the children (see below).

The activities of these companies has meant that UK government data, covered by the Official Secrets Act, has been removed from the country, including Parliamentary data - ask Microsoft, they handle the House data. The number of people in the UK whose data has been stolen is approximately 38 million, 67% of those 57 million people in the UK, who use the above company's services on the web. Amongst the data stolen is the data of about 1.5 to 3 million children between the ages of 3 and 17. That data is now stored in the files of a foreign intelligence agency; permanently, for the duration of those children's lives; un correctable, un amendable.

Please do not put British companies in this position.

Kevin Cahill

11 January 2016

Duncan Campbell—written evidence (IPB0069)

My name is Duncan Campbell. I am an investigative journalist and a registered court expert witness on communications and computer data.

I write to offer evidence and to give oral evidence if requested to your Committee on the Draft Investigatory Powers Bill proposals in areas of which I have specialist knowledge or experience.

I gave evidence[182] in October 2012 to the Joint Committee then reviewing the Draft Communications Data Bill, and on which the government did not proceed. Further and fuller details of my work and experience over the past 35 years are at the end to this note.

I would also offer to assist in supporting evidence to be provided to the Committee by Mr William Binney, formerly of the United States National Security Agency. I have worked with Mr Binney during the course or the last six months so as to assess and report on the applicability and relevance to the UK of technical methods and approaches developed while he was a Technical Director of the NSA, particularly in regard to minimising intrusion within lawful boundaries and consequently improving operational efficiency in respect of bulk collection.

These matters also have specific and direct relevance to the potential for the general protection of Parliamentarians' communications (and the communications of other protected professions, such as lawyers) from random and unlawful intrusions as a result of unconstrained bulk collection.

This is a matter on which I reported shortly before this Bill was introduced in November this year. The gist of my report was that the Investigatory Powers Tribunal had in 2015 been misled by the government side as to the practicality of restraining collection of MPs' and Peers' communications within the apparatus of bulk collection, [183] pursuant to the long-established Wilson doctrine.

I have studied and assessed extensive further material relevant to the contention that excess interception and overcollection has prejudiced security by drawing focus and resources from potential directed intelligence or human intelligence operations against identified suspects onto almost incomprehensibly large systems of general population surveillance.

There are abundant examples of this in many now published studies and reports of the U.S. National Security Agency, for which Mr Binney worked. Even as early as 2006, NSA colleagues reported that:

---

182 www.parliament.uk/documents/joint-committees/communications-data/Oral-Evidence-Volume.pdf#page=301

183 http://www.theregister.co.uk/2015/11/04/gchq_smart_collection_nsa_man_bill_binney

> "Everyone knows that **analysts have been drowning in a tsunami of intercept whose volume, velocity and variety can be overwhelming**."[184]

There are also examples of how directed or intrusive surveillance, as opposed to bulk collection, has been the primary means of detecting and preventing both terrorist activities and conspiracies to abuse children.

I have more recently reported on the previously wholly secret aspects of the development over the last 15 years of general multiple mass linked databases on the entire population or sub-populations as a means of "enrichment" of communication data analyses. [185] Some of these have now been avowed, but the nature of most information has not been identified to the public or Parliament generally.

This includes the implications of the creation of a permanent national telephone call and Internet connection records database, held secretly by the government, and which was not avowed until the day this bill was presented in Parliament.

I have referred in my report to the role of the seldom-mentioned intelligence support agency NTAC (the National Technical Assistance Centre) in acquiring personal bulk information databases by overt and covert means, the majority of which remain undeclared and unjustified to Parliament, notwithstanding admissions that have been made.

A grave effect of this admission is that Parliament has been extensively and repeatedly misled over the past 15 years by statements which can now be seen to be inaccurate about the need for and unavailability of historical call data records. This has also to my knowledge prejudiced police investigations and prosecutions, as well as the proper defence of accused persons in serious criminal cases. In such cases, which may well have involved lengthy and repetitive police enquiries over many months before arrest, charge and trial, senior investigation officers and/or defendants' legal representatives have been told by telecommunications companies that data is not held and is destroyed after the retention period of up to one year.

It is now apparent that this was a charade, in that all communications data was collected, retained and analysed nationally in a process quite separate to the authority Parliament provided under RIPA.

Like many others who wish to assist the Committee, I have been impaired in being able to assess and consider the Bill's provisions and its implications for the next decade or more. It would be of immense assistance to mature and productive discussion, and to Members' scrutiny, if significantly more time were made available within the Parliamentary timetable I have watched as successive Bills at 15 year intervals have obfuscated or failed to address technological and legal issues. This is the largest bill ever, and has brought hitherto clandestine activity affecting every voter into the open. It merits careful reflection.

---

[184] https://www.eff.org/files/2015/05/26/20150505-intercept-sidtoday-tsunami-of-intercept-final.pdf (emphasis added)

[185] http://www.theregister.co.uk/2015/12/16/big_brother_born_ntac_gchq_mi5_mass_surveillance_data_slurping

Noting the shortness of time and the Committee's timetable, I intent within that limit of time to provide further examples and assessments relevant to the questions the Committee has laid out.

Duncan Campbell

PERSONAL EXPERIENCE AND INVESTIGATIONS

Between 1976 and the present, I have identified and framed important issues concerned with communications intelligence and surveillance for Parliament and the public, and for the European and international communities.

I described and brought to general attention surveillance arrangements and facilities which successive British governments have planned and/or operated contrary to UK or international law, and/or outwith law generally, and/or without due accountability to Parliament and the Courts. These reports have resulted in official investigations, judgments and legislative changes over three decades.

My reporting in 1980 led directly to the passing of the Interception of Communications Act 1985,[186] and to the creation of the offices of the Interception of Communications Commissioner and the Interception of Communications Tribunal.[187] His reporting in turn contributed to the passing of the Security Services Act 1989,[188] the Official Secrets Act 1989,[189] and the Intelligence Services Act 1994.[190] These brought the separate branches of the intelligence and security services within the remit of statute law and created formal mechanisms for accountability, including the formation of the Parliamentary Intelligence and Security Committee. The process continues to this day.

Since 1979, and in particular since 2002, I have worked as a forensic expert witness in major terrorism and other serious criminal cases in the Britain and Ireland In these cases, I has been employed to analyse, audit and report on large quantities of complex communications and computer data disclosed under the provisions of RIPA.

I have provided evidence concerning communication interception and communications data to the Court of Appeal,[191] the Supreme Court,[192] the Interception of Communications Tribunal, and the European Court of Human Rights, as well as to Crown and other UK Courts. The cases have included the use of communications data and communication interception evidence from overseas jurisdictions admitted in UK criminal proceedings.

---

186 1985, chapter 56.

187 *Ibid*, sections 7 and 8.

188 1989, chapter 5.

189 1989, chapter 6.

190 1994, chapter 6.

191 R v Winters [2008] EWCA Crim 2953; [2008] WLR (D) 387, R v Breton [2008] EWCA Crim 2935, Clifford v Herts [2008] EWHC 2549, Clifford v Herts [2008] EWHC 3154, R v Iqbal [2009] EWCA Crim 1627, Clifford v Herts [2009] EWCA Civ 397, Clifford v Herts [2009] EWCA Civ 1259.

192 R v Austin & ors, Supreme Court [2009] EWCA Crim 1527.

In 1998, I was appointed a consultant to the Scientific and Technological Options Assessment (STOA) office of the European Parliament and asked to prepare a report on communications surveillance and communications security. The European Parliament published my report "Interception Capabilities 2000",[193] in April 1999.

In January 2001, I provided further reports on communications intelligence to the European Parliament Temporary Committee on the ECHELON interception system.[194] The committee made substantial recommendations to curb and restrict communications surveillance for the purposes of the protection of human rights and of European commerce. The recommendations were passed in their entirety by the European Parliament on 5 September 2001. [195]

From October 1999 to June 2000, I was a senior research fellow at the Electronic Privacy Information Center (EPIC), Washington DC. I there prepared a report intended for the United States Congress on the satellite communications interception arrangements known as "Echelon."[196]

Between 1999 and 2002, I testified and provided reports on communications intelligence and interception to the national Parliaments of Denmark, Germany, Japan, the Netherlands, and Sweden and to the intelligence supervisory committee of the Belgian government.

I was instructed by Liberty and Keir Starmer QC (later the DPP and now MP), as the expert witness for the applicants in ICT hearings and the subsequent ECHR case on filtering and communications surveillance using bulk data, *Liberty v UK*. [197]

In its judgment issued in 2008, ECHR held that United Kingdom law did not provide "adequate protection against abuse of power" in respect of bulk data. The Court criticised the "very wide discretion conferred on the State" to intercept and examine bulk communications.

Although found in breach of Article 8 and ordered to pay damages, the United Kingdom government omitted to enact legislative changes on the basis that the Interception of Communications Act 1985 had been superseded by RIPA by the time of hearing and judgment. I am aware that the Committee's remit considers whether the breach of Article 8 will be remedied by the proposed Bill.

---

193 http://www.europarl.europa.eu/RegData/etudes/etudes/join/1999/168184/DG-4-JOIN_ET(1999)168184(PAR01)_EN.pdf

194 http://home.datacomm.ch/Ibernasconi/repository/texts/echelon.europa/7747.html, http://home.datacomm.ch/Ibernasconi/repository/texts/echelon.europa/7752.html, http://www.europarl.europa.eu/meetdocs/committees/temp/20010322/433524EN.pdf

195 http://europa.eu/rapid/press-release_SPEECH-01-368_en.pdf?locale=en, http://www.european-security.com/index.php?id=784.

196 See www.duncan.gn.apc.org/EPIC_2000.pdf .

197 Liberty, British Irish Rights Watch and the Irish Council for Civil Liberties ("Liberty and others") v the United Kingdom, 48 ECHR 1.

In May 2015, I was invited to open a conference on Intelligence, Security and Privacy held at Ditchley Park in conjunction with the new director of GCHQ, Mr Robert Hannigan.[198]

Further details of key issues and reports affecting communications data

The matters reported and briefly described below are material to issues which arise in the draft Investigatory Powers Bill, including compliance with privacy and other legislation, financial probity, the ability of citizens to understand and anticipate the effects of legislation, the role of filtering systems, and the concealment of projects and technical arrangements from Parliamentary oversight.

- GCHQ

  Issue – activities of the intelligence services unacknowledged to Parliament, unaccountable and operating outside the framework of statute law.

  In 1976, I and a co-author published the first article to describe the nature of communications surveillance activities conducted by Government Communications Headquarters (GCHQ). At the time GCHQ was not known to Parliament or the public, nor acknowledged as an intelligence agency, although it was, then as now, the largest of Britain's intelligence services. The "Eavesdroppers" report was controversial throughout the latter 1970s.[199]

  The publication led to internal reviews in which the Legal Adviser to the Foreign Office minuted *inter alia* that "it now seems clear that [the interception of foreign embassies' communications, as the article described] is at least a dubious practice."[200]

  Subsequently, GCHQ's activities were formally acknowledged and placed under statutory supervision by the Intelligence Services Act 1994.

- Telephone tapping

  Issue - prior to 1985 telephone tapping (interception) in the UK was conducted without statutory legal authority and contrary to ECHR.

  In 1980, I published reports describing the scale and technical arrangements for telephone tapping activity in the United Kingdom.[201] The report led directly to a

198 http://www.ditchley.co.uk/conferences/past-programme/2010-2019/2015/intelligence

199 "The Eavesdroppers", Time Out (London), 21 May 1976. See www.duncan.gn.apc.org/ Eavesdroppers_1976.pdf.

200 Sir Arthur Hockaday to D of HQ Sy, 27 June 1978, PRO file DEFE 47/34; cited in Richard G Aldrich, *GCHQ*, Harper Press 2012, pps 360 and 599.

201 See www.duncan.gn.apc.org/Interception_1980.pdf.

Home Office white paper instituting supervision arrangements for interception for the first time.[202]

My 1980 reports, and his subsequent provision of technical evidence to the European Court of Human Rights on "printer metering" (the earliest form of communications data) in the case of *Malone* led to an ECHR judgment finding the United Kingdom in breach of Article 8. The Court found that UK law failed to 'indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities". [203] This is the historical antecedent to the contemporary and arguably no longer relevant split between content and metadata.

- Interception of commercial satellite communications *(Echelon)*

  Issue – from 1969 on, the United Kingdom created and participated in a clandestine program to intercept all commercial satellite telecommunications, including the communications of all UK private citizens and businesses, as well as those of allied countries.

  In 1987, I published a report describing the nature of international communications satellite surveillance activities conducted by GCHQ in collaboration with international partner agencies. The activity, known as "Echelon", has not been described or publicly acknowledged to Parliament.[204]

  The first known type of communications content and data filtering was developed for the Echelon project in 1969. The system initially used early computers to process and filter intercepted communications data using lists known as "Dictionaries". [205] These continue to be used to this day.

  Although extensively examined by the European Parliament and national Parliaments, the legality of the Echelon system and the role of Echelon dictionaries in filtering communications has not been tested before the ECHR or in other fora.

- Communication intelligence satellite constructed without parliamentary authority *(Zircon)*

  Issue – during the 1980s, GCHQ obtained ministerial authority to spend £500 million to acquire a proposed signals intelligence satellite without advising the Public Accounts Committee.[206]

---

202 `The Interception of Communications in Great Britain', Cmnd 8191, March 1981.

203 Malone v United Kingdom (1984) 7 EHRR 14.

204 See www.duncan.gn.apc.org/Echelon_1988.pdf.

205 Aldrich, *op cit*, pps 342-344.

206 See www.duncan.gn.apc.org/zircon_1987.pdf.

Notification had been required under a parliamentary agreement resulting from previous concealed overspending on the Polaris missile improvement program known as "Chevaline".[207]

I reported on the satellite project, known as Zircon, for the BBC and in the press.[208] The BBC report was initially withheld on government request but was transmitted in 1988.

- Unlawful Interception of telecommunications *(Liberty v UK)*

  Issue – between 1990 and 1997 all communications to and from the Irish republic were intercepted and processes at a specially constructed facility in Cheshire, using "filtering" to extract content and data of interest.

  The normal arrangements for interception of communications in the period were that British Telecom would be served with a warrant under IOCA, and would make necessary technical arrangements. Exceptionally, the wholesale interception of all communications in Cheshire was carried out without BT co-operation in the normal way.

  The arrangements at the Cheshire facility (the "Capenhurst tower") involved obtaining the content and addresses of telephone calls, faxes and emails. These were stored and filtered before being transmitted to users by optical fibre cables.

  The operations at the Capenhurst tower were at the centre of the *Liberty v UK* case before ECHR, as described above. The Court found that the filtering procedures, described by government witnesses as "drawing down", did not set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material. State interference with the applicants' rights under Article 8 was therefore found not to be "in accordance with the law".

Biographical

I graduated in physics from Oxford University in 1973 and further trained in Operations Research at the University of Sussex. I was a consultant on Telecommunications to the Technology Faculty of the Open University and in that capacity co-wrote a textbook on "The British Telephone System" for the University's Systems Behaviour course. I am a member of the Institute of Telecommunications Professionals (ITP) and a Fellow of the Royal Society of Arts. I am a visiting fellow and lecturer at the Media School of Bournemouth University.

21 December 2015

---

207 Ninth Report from the Public Accounts Committee, Session 1981-82, Chevaline Improvement to the Polaris Missile System, HC 269.

208 See www.duncan.gn.apc.org/zircon_1987.pdf.

Duncan Campbell—supplementary written evidence (IPB0124)

This is a supplementary note of documentary material and questions relevant to the committee's review, supplementary to my evidence note of 19 December 2015. My experience and involvement with the matters before the Committee is recited there.

"Internet Connection Records" (ICR) are already created and held

A major issue which may arouse concern with the form of the draft legislation is that the "Internet Connection Records" (ICR) which the Bill proposes should in future be created and retained by Service Providers are already created directly by government agencies and are held, systematically and on massive scale. As of 2012, provision had been made for the storage of 24 trillion (24 thousand billion) such records.[209]

These records include metadata and extensive further metadata derived from analysis of content concerning all types of internet connection, in relation to the totality of UK internet users, all of which is available for any form of analysis and extraction without warrant by UK agencies and by foreign partners. The basis of and sources for these factual statements is described following.

The Committee has asked, *inter alia*:
• Is accessing Internet Connection Records essential for the purposes of IP resolution and identifying of persons of interest?
• Are the requirements placed on service providers necessary and feasible?
• Are the powers sought necessary?
•Has the case been made, both for the new powers and for the restated and clarified existing powers?
• Are there alternative mechanisms?

Given the published facts, the answer to the committee's final question appears to be "yes". ICR (as defined) are currently obtained and generated at the rate of many billions per hour from bulk communications data processed and analysed by GCHQ using a small number of warrants issued under Section 8(4) of RIPA, and have been so obtained since at least 2008.

These Internet Connection Records are derived from a network of probes connected to submarine optical fibre communications cables as they enter and leave the United Kingdom through shore terminal stations, and which existing service providers have been compelled to install by virtue of technical orders made under RIPA and the Telecommunications Act 1984.

The Internet communications data obtained is refined by a process known as "sessionisation". Sessionisation re-assembles the data packets making up individual communications. The technology for sessionisation for Internet optical fibre

[209] https://theintercept.com/document/2015/09/25/gchq-analytic-cloud-challenges Page 6

communications was first developed by an NSA team led by Mr William Binney, whom the Committee have invited to give oral evidence.

I have worked with Mr Binney to examine the UK material employing this type technology, and to consider its relevance to the question of whether Internet Connection Records are in fact necessary given existing deployments. It appears from the UK documents that they cannot be necessary, in that (on the evidence published and cited here) they are already available now (and are filtered) in a far more powerful form than any UK service provider would be able to achieve in the future.

It would follows that the requirements proposed in the draft Bill to be placed on service providers cannot be necessary, whether or not they are in fact feasible to be carried out at the ISP level, or are judged proportional.

There is now abundant evidence that Internet Connection Records of the type proposed to be created and held for Law Enforcement and other purposes already exist and are collected on a massive scale by GCHQ, and that this activity has been taking place since at least 2008. The largest part of this evidence is a corpus of 28 GCHQ documents published by the U.S. online magazine, The Intercept, on 25 September 2015.[210] The documents accompanying the article were, according to the magazine, published in so as to highlight the scope of existing investigation systems installed within the UK Internet, and in anticipation of the expected new legislation.

I would respectfully suggest that the 28 GCHQ documents as a group merit at least the same attention as the Home Office publications accompanying the Bill, for the reason that the GCHQ documents extensively and helpfully explain and define technical and legal practices in the areas to be legislated, as they exist now and as they have evolved over the past 15-30 years.

One GCHQ document in particular, entitled "Operational Legalities", runs to 156 pages and is one of several providing extensive guidance as to current legal practice.[211] One matter of particular concern as to proportionality is current guidance indicating that the all forms of metadata concerning communications between persons in the UK (such as e-mail addresses, e-mail headings, messages, etc, and also including locations and passwords) and taken into GCHQ repositories may currently be examined and analysed without restriction, and without the need for a targetted warrant.

As of 2012, according to a report on "GCHQ Analytic Cloud Challenges" [212], Internet Events records were then being recorded at the rate of 50 Billion Events Per Day, with a capacity

---

[210] https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities
[Declaration of interest: I have written a report for The Intercept.]

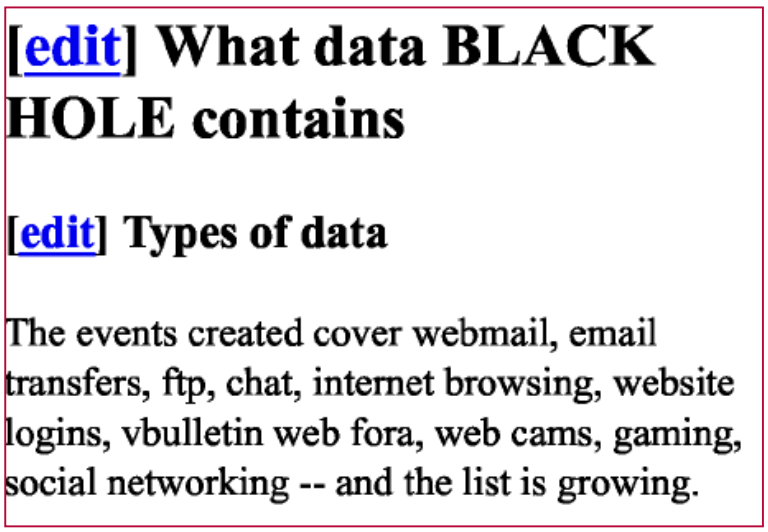
[211] https://theintercept.com/document/2015/06/22/operational-legalities-gchq-powerpoint-presentation;
https://theintercept.com/document/2015/09/25/pull-steering-group-minutes;
https://theintercept.com/document/2015/09/25/content-metadata-matrix;
https://theintercept.com/document/2015/09/24/legalities

[212] https://theintercept.com/document/2015/09/25/gchq-analytic-cloud-challenges

then to rise to double that amount. These records included all Internet activity with one or both terminals in the UK, as well as Internet communications events passing through the UK. In 2012, this is said to have included 15 Billion web visit record per day. Each record is an Internet Connection Record, in that it includes all available metadata information about users, their locations, their identifiers and addresses, as well as times and dates and services used, and the user identifiers within their services.

ICR Records and filters in BLACK HOLE data and applications

According to the published documents, the Internet records are accumulated and stored in two depositories in Bude and Cheltenham, named "BLACK HOLE ". The records are then accessed and processed by filters, resulting in the creation of multiple datasets or databases directly capable of answering all the matters set out in the ICR Operational Requirements statement for the Investigatory Powers Bill.[213]



[edit] What data BLACK HOLE contains

[edit] Types of data

The events created cover webmail, email transfers, ftp, chat, internet browsing, website logins, vbulletin web fora, web cams, gaming, social networking -- and the list is growing.

Published GCHQ description of BLACK HOLE Internet Connection Records. [214]

In particular, as shown above, the ICR type of records already contain the "who, when, what, how" type of information that Parliament has been told is currently a "gap" in capability. It follows from this evidence that it may waste public funds, and place an unneeded burden on service providers, to require forced duplication of existing and inferior capabilities.

The sample of requirements for ICR, set out on page 25 of the draft Bill, lists three matters, each of which are shown by the 28 GCHQ documents to already exist in a comprehensive way, providing information far beyond that which service providers do hold or could reasonably be expected to create and retain in future.

The sample suggested requirements were:

---

[213] GCHQ's documents sometimes use different names to the Home Office. Internet Connection metadata records held in BLACK HOLE are called "Single Line Records". The Filter or Filters are generally described as "Query Focussed Datasets". These are databases created when filters are applied to BLACK HOLE raw data.

[214] https://theintercept.com/document/2015/09/25/data-stored-black-hole

(1) To establish what services a known suspect or victim has used to communicate online, allowing investigators to request more specific communications data;
(2) To establish whether a known suspect has been involved in online criminality, for example sharing indecent images of children, accessing terrorist material or fraud;
(3) To identify services a suspect has accessed which could help in an investigation including, for example, mapping services;

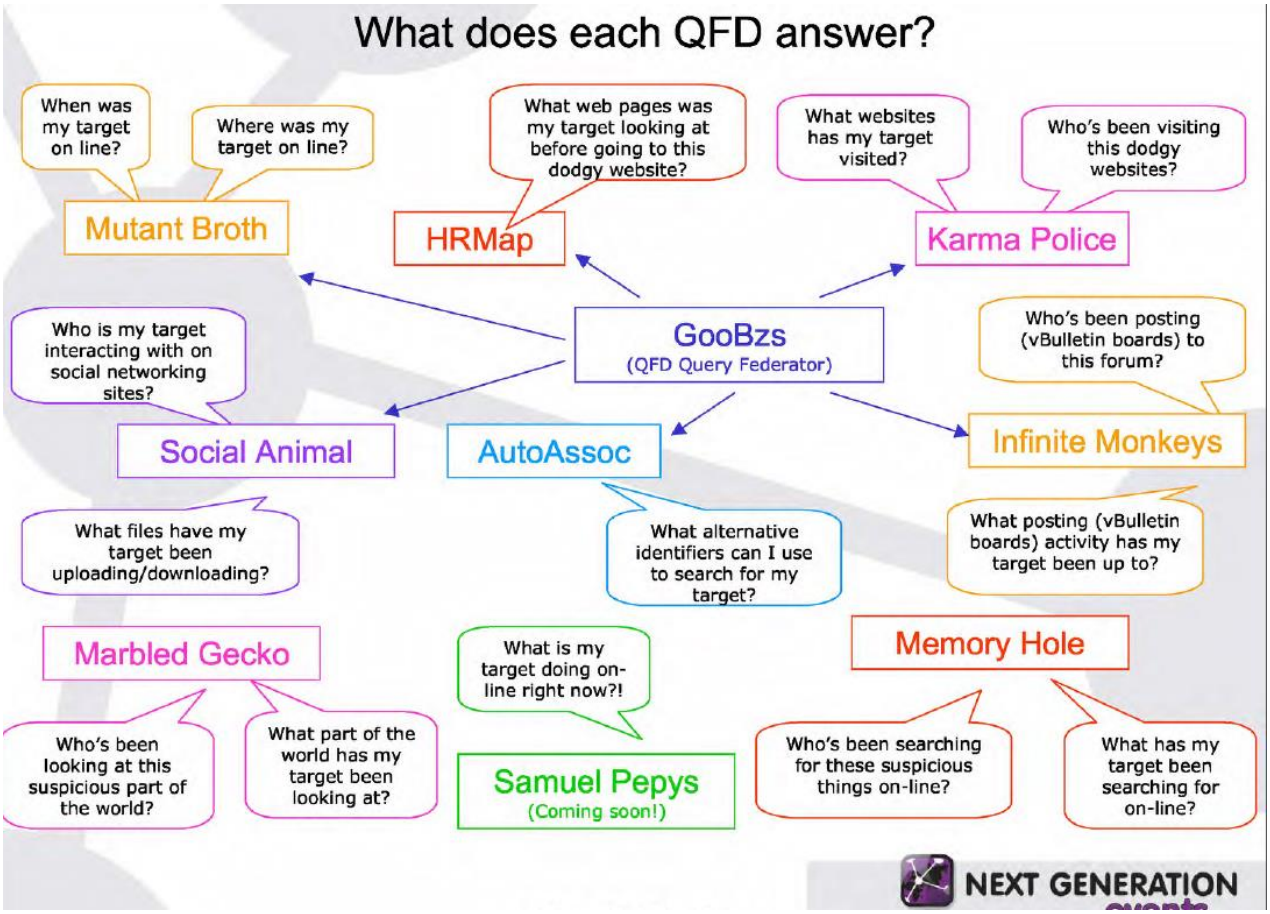
The table below appears in the published GCHQ Analytic Cloud Challenges report (foot notes 1 and 4, *supra*), page 5. It demonstrates that all of the questions raised in the ICR are currently answered by the BLACK HOLE system of data and queries.

Name			
AUTOASSOC	Bulk unselected TDI-TDI correlations with confidence scores.	What other TDIs belong to your target ? What technologies your target is using ?	2+1 instances, each 50-70TB storage
Evolved Mutant Broth	Identify when certain TDIs appear in traffic which indicate target usage and their location. Telephony and C2C data provide a converged view.	Where has my target been? What kind of communications devices has my target been using?	10+5 instances, each 70TB storage
Hard Assoc	Provide strongly correlated selectors for both C2C and Telephony traffic taken from TDIs appearing in the same packet	Are there any alternative C2C or Telephony selectors for my target?	3+2 instances, each 70TB storage
HRMap	Host-referrer relationships - information about how people get to websites, including links followed and direct accesses.	How do people get to my website of interest and where do they go to next? What websites have been visited from a given IP?	5+3 instances, each 70TB storage
KARMA POLICE	Which TDIs have been seen at approximately the same time, and from the same computer, as visits to websites.	Which websites your target visits, and when/where those visits occurred. Who visits suspicious websites, and when/where those visits occurred. Which other websites are visited by people who visit a suspicious website. Which IP address and web browser were being used by your target when they visited a website.	11+7 instances, each 70TB storage, 3+1 correlator instances
SOCIAL ANTHROPOID	Converged comms events allowing you to see who your targets have communicated with via phone, over the internet, or using converged channels (e.g. sending emails from a phone or making voice calls over the internet).	What communications your target is engaged in. Who has your target been communicating with. What communications have occurred using a particular locator (IP address, cell tower, etc).	6+3 instances, each 70TB storage

From GCHQ Analytic Cloud Challenges report , page 5

Specified and comprehensible examples of how this type of information directly provided answers to the concerns raised are shown in a further table overleaf identifying the filters, or "Query Focuses'" which extract the relevant data from BLACK HOLE. [215]

[215] https://theintercept.com/document/2015/09/25/demystifying-nge-rock-ridge page 4



From "Demystifying NGE Rock Ridge" page 4

For example, the question "What web pages was my target looking at before going to this dodgy website?" is answered by the filter (or "QFD") HRMAP. The question "What websites has my target visited?" is answered by the filter KARMA POLICE. These would include identifying users who had visited sites offering indecent images of children, or sites offering terrorist materials.

An inquiry to identify services a suspect has accessed which could help in an investigation including, for example, mapping services would be answered by the MARBLED GECKO filter, which records data answering questions such as "Who's been looking at this suspicious part of the world?" or "Find out who has been looking at what on Google Earth".

According the documents the GCHQ KARMA POLICE filter or QFD "aims to correlate every user visible to passive SIGINT with every website they visit, hence providing either (a) a web browsing profile for every visible user on the internet or (b) a user profile for every visible website on the internet." It appears from the reports to hold precisely the material about "what services a known suspect or victim has used to communicate online" that is claimed to be unavailable, and to have done so for at least five years.

Other filtered data derived from BLACK HOLE hold bulk data concerning bulletin board use [INFINITE MONKEYS], Social Networking Site activity [SOCIAL ANIMAL], and search engine requests [MEMORY HOLE].

The information which can be used to identify and access the filtered records includes, according to the documents "web service authentication data", "ID card number or passport number", "driving licence number", "car registration number", and/or "bank card/credit card account numbers".

The existing BLACK HOLE system is on this evidence already more capable than the ICR records system proposed in the Bill. For example, as shown above, a filter or "QFD" called SAMUEL PEPYS will answer the question "What is my target doing on- line right now?".

To my knowledge or in my understanding, all of the internet connection records systems creating the UK's BLACK HOLE repository are built on the Internet fibre cable sessionising systems which Mr Binney's US team devised and which he has explained to the Committee.

Despite the recent disclosures about and avowal of bulk data collection from the Internet, there has been a marked by the government to disclose that the requirement for Internet Connection Records has already been achieved for some time, but that the data recovered has not been made available to law enforcement.

I will be glad to further assist the Committee on any of these matters.

Duncan Campbell

22 December 2015

Lord Carlile of Berriew CBE QC—written evidence (IPB0017)

1. This is my personal submission to the Committee concerning the draft Bill. In this paper I do not attempt to cover all the issues raised in the Bill, but rather deal with those of particular concern to me. I would be happy to deal with additional issues if required.

Relevant interests.

2. From 2001-2011 I was the Independent Reviewer of Terrorism Legislation. I am DV vetted.I remain the non-statutory reviewer of national security arrangements in Northern Ireland. I was one of 3 commissioners appointed in 2015 to consider and comment on a report by the relevant authorities in Northern Ireland concerning the activities of organisations formerly and/or currently involved in terrorism: this work was requested and completed following the breakdown of power sharing in the Belfast Legislative Assembly.
3. For completeness, I add that I am a director of SC Strategy Ltd, a strategy consultancy which I run with Sir John Scarlett KCMG OBE (former Chief of MI6) and Lord Arbuthnot of Edrom. One or two media stories have suggested that we work operationally in the areas of intelligence and counter-terrorism. In fact this is not correct. We do provide advice to clients on the risks posed by cyber-activism, and related issues.

Necessity of powers for the security and intelligence services and law enforcement. General points.

4. My view and advice is that it is essential that good access to communications data is retained. This is founded not merely on issues relating to terrorism. It is also vital in dealing with other serious crime, organised crime, money laundering and sexual exploitation. The role of the State in reducing privacy is much exaggerated: most users of the electronic world have surrendered a significant proportion of their privacy to the private sector, which has access to and trades routinely in huge amounts of personal information, far more than the State would ever want. Nevertheless, there is sufficient concern about the possible misuse of personal information and legitimate privacy by the State, for this to beexamined closely. State access should be kept to the minimum compatible with the public interest.
5. For the security and intelligence agencies [SIAs] and the police, their ability to carry out their job effectively relies on access to the available powers, sometimes at short notice.
6. The Security Service [MI5] are correct in saying that communications data has played a key role in all their investigations over the past decade. I have seen raw evidence of this.
7. The Independent Surveillance Review [ISR] produced by RUSI reported:

> *'Data interception is fundamental to the work of GCHQ and forms an essential part of its tradecraft. Whereas in the past it was relatively*

straight forward to intercept telephone data, the job of data interception is now more complex.'

8. Flexibility for the future should take the increasing complexity into account. Communications are increasingly moving from telephony to internet-based data. By way of examples:
    i. WhatsApp – 900m monthly users (Sep 2015). Facebook 1bn users in a day (Aug 2015).
    ii. 1 March 2015: within the UK, 23% of internet users were regular users of Voice Over Internet Protocol (VoIP) services; 30% of 16-24yr olds; 28% of 25-39yr olds (YouGov).
    iii. Standard and multimedia messaging service [SMS/MMS] is decreasing in UK: 2009: 106bn; 2012: 151bn; 2014: 110bn (Ofcom, 2015).
9. Communications data has been used in every Security Service counter terrorism operation over the last decade; and in 95% of serious crime trials prosecuted by the Crown Prosecution Service [CPS]. I can give examples of cases in which I have appeared as an advocate.
10. In particular, cell-site analysis is used in most serious criminal cases where the defendant has pleaded not guilty.
11. Investigation of complex cases can be a slow process because criminals often cover their tracks.
12. To ask communications service providers [CSPs] to hold data for 12 months is very reasonable – less time would be inadequate. In my view a longer retention period would be defensible, and probably advisable, in the public interest.

Targeted and Bulk Interception.

Are there sufficient operational justifications for undertaking (a) targeted and (b) bulk interception?

Targeted.

13. Current operational justifications are sufficient evidence for targeted interception. These are:
    a. The interests of national security;
    b. The prevention and detection of serious crime;
    c. Safeguarding the economic well-being of the UK (amounting to national security).
14. I have reflected on the question of whether those justifications are too ambiguous? In particular, I have considered the elasticity of the term 'national security'. National security is not defined by UK or European law. A benefit of the absence of a proscriptive definition is adaptability. However, it is said that it can be exploited, politicised and thereby degraded.
15. I have heard cited as an example of such degradation the interception by US

authorities of the telephone calls of Chancellor Angela Merkel. However, I am extremely dubious that authorisation for such interception in the interests of national security would ever be given in the UK. Indeed, I doubt the lawfulness of that particular interception under the relevant US law.

16. I consider that 13(a) and (b) above should present no difficulty.

17. How clear are the criteria of safeguarding the economic well-being of the UK? They are not, if judged by the canons of statutory interpretation. However, defining them would be extremely difficult. They would certainly encompass the continuity of the National Grid and of the mobile telephony system, as well as the integrity of bank to bank communications. Possibly a non-exhaustive list of examples might be produced in a statute: I believe this would provide helpful guidance.

18. In principle, the safeguarding of the economic well-being of the country is surely a classic matter for Ministers, acting on advice from the relevant Government sources? We have to work on the assumption that an elected government broadly can be trusted, given Parliamentary accountability. I know of no evidence at all to justify concern about the use of proportionate Ministerial judgement and discretion in relation to economic matters.

Bulk.

19. Like targeted interception, the justifications for bulk interception are:

    a. National security;

    b. Prevention and detection of serious crime;

    c. Safeguarding the economic well-being of the UK as it pertains to national security.

20. National security must remain a statutory purpose when a warrant is sought for collection of material in bulk.

21. Due to the nature of bulk interception, and the wide net of information that is intercepted, there should be greater understanding in this context of 'safeguarding the economic well- being of the UK'. Whilst I am opposed to a statutory definition, the Committee would be entitled to look for more clarity as to the process whereby this criterion is certified, and who is involved. It would be reasonable for HM Treasury to be required operationally in each case to certify that the issues under consideration reached the high standard implied by the test.

22. According to the ISC Report, Bulk interception is used for 2 reasons: (1) to investigate the communications of individuals already known to pose a threat; and (2) to generate new intelligence leads, for example to find terrorist plots, cyber-attacks or other threats to national security.

23. It is a positive element that bulk interception warrants must set out the specific purposes which must be met before any of the data that has been collected can be examined.

24. It is positive that the application for bulk interception warrants continue to be limited to the SIAs.

25. It is a sound principle that, if the information can be obtained by another, less

intrusive method, that method should be employed. However, perhaps more clarity is required as to the assessment of the capability to acquire information by other means. For example, if it were possible to acquire the information via intelligence obtained lawfully from individuals, but at high risk, would that be defined as unobtainable? The Committee's report may be able to provide some persuasive reflections on this issue.

Are the proposed authorisation processes for such interception activities appropriate? Is the proposed process for authorising urgent warrants workable?

26. I have some concerns about the proposed authorisation processes.
27. In principle the issue of warrants should be for Ministers alone. They have the material information available at all times. They can be briefed fully by officials from all relevant parts of government, with impartial advice provided in their private offices. On potential Parliamentary issues, they can take the advice of their Parliamentary Private Secretaries if appropriate.
28. Ministers are accountable to Parliament. This includes accountability to Select Committees, to the relevant House, and ultimately to their electorate. Ministers seen to be inefficient or troublesome can be reshuffled at short or even no notice.
29. It is not the normal or even acceptable role of a judge to make executive decisions. They are not elected, and rarely removed.
30. The muddying of the separation of powers is illustrated starkly by ample evidence of judicial partiality in some of the States of the former Soviet Union, the Balkans and elsewhere.
31. If judges are to be involved in warrantry, indubitably it will raise questions of the separation of powers being compromised – of the red line being crossed by judges making what constitutionally are executive decisions.
32. We have to be frank about this aspect of the proposals. Because there is a degree of mistrust (in my view misplaced) of the SIAs and (generically) Ministers, an additional layer of verification is seen as necessary.
33. It is all too tempting to regard judges as a readymade solution to form that layer. However, there is the danger of pragmatic incrementalism, by which judges are given increasing roles outside their proper range, and well outside their daily competencies.
34. Whilst reluctantly I am prepared to accept the involvement of judges as provided in the draft Bill, I hope that the Committee will recognise that the judicial responsibility should be only one they are fully qualified to undertake. Therefore, it is important that judges are properly trained in national security practice, the nature and detection of terrorism and other issues relevant to warrantry applications.
35. Further, judicial activity should be confined to what are properly judicial roles. This is why the Government is correct in its view that Judicial review principles should apply. The proper question is whether the Minister acted lawfully in issuing the warrant, not whether the judge agrees with the issue of the warrant: the latter question clearly would place the judge in the position of a Minister. Judicial Review principles are familiar to the judiciary, and are based on well understood principles founded on reasonableness and proportionality.

36. Within the above reservations, the proposed double-lock authorisation is acceptable.
37. The authorisation of urgent warrants is limited firmly in the proposals. It can be given orally by the Secretary of State, and must be reviewed by a Judicial Commissioner who will have the power to quash a warrant on the same principles as with other warrants.
38. I suggest that there should be Guidance Notes as to what constitutes an emergency – for example, referring to how imminent the perceived threat is, the level of threat etc. The issuance of an urgent warrant should be accompanied by a note recording the criteria and reasoning applied. This will facilitate review, and confirmation where appropriate.
39. I can envisage an emergency situation in which not all the legal criteria of legality could be met, but clearly a Minister would be unwise not to issue a warrant. An example of this might be a potentially immediate and large scale threat to life disclosed through a source not generally regarded as reliable. Such a decision may be sound and even essential for the protection of national security. The provisions should envisage that Ministers acting in good faith are not seen to have acted unlawfully in such situations. They would probably be protected under Judicial Review principles, but some clarity would be welcome either in the legislation or in Guidance Notes.

Communications Data.

Are the definitions of content and communications data (including the distinction between 'entities' and 'events') sufficiently clear and practicable for the purposes of dealing with such data?

40. In paragraph 9 above I have described briefly the importance of communications data across a wide range. There is no doubt that many serious criminals have been convicted by communications data, which is objective evidence generally incapable of contradiction.
41. I believe that the definitions are accurate and sufficient.
42. The data containing the characteristics of communication data (often called the metadata) can in my view be distinguished without difficulty from the content of the communication. If appropriate and defined protocols and guidance are adopted, there should be a negligible risk of straying from the characteristics into the content.
43. In many cases the characteristics of the data will provide more compelling evidence than the content. The metadata does not lie: the content may do so, often deliberately.

Are there sufficient operational justifications for accessing communications data in bulk?

44. It would be useful, where possible, to see further information about the successful uses of bulk communications data collection to be published, for the benefit of UK population.
45. Bulk collection is to be permitted when it is necessary for the protection of

national security. It is a positive step that warrants are introduced for the collection of communications data in bulk.

46. The data is only accessed where necessary and proportionate, to enable the SIAs to carry out their statutory function – it cannot be accessed for other purposes. This is a reasonable limitation.

Is the authorisation process for accessing communications data appropriate?

47. For the SIAs, the ability to perform their job effectively depends upon these powers and access to the data.
48. Communications data has played a key role in all MI5 investigations over the past decade.
49. The ISR reported that data interception is fundamental to the work of GCHQ and forms an essential part of its tradecraft. Whereas in the past it was relatively straight forward to intercept telephone data, the job of data interception is now more complex: see paragraph 8 above.

Equipment Interference.

Should the SIAs and law enforcement have access to powers to undertake (a) targeted and

(b) bulk equipment interference? Should law enforcement also have access to such powers?

50. Such powers should be available to SIAs and law enforcement for targeted equipment interference.
51. Whilst it is right that legal limitations cannot realistically be placed on encryption, which is used for reasonable and lawful commercial purposes, in my view it is necessary that powers are in place. This will help the authorities, in a targeted situation, to combat the increasing use of encryption, especially by those who threaten UK national security.

Are the authorisation processes for bulk interference activities appropriate?

52. The proposed safeguards appear appropriate, in particular the 'double lock' authorisation procedure. Whether bulk interference is necessary and proportionate will be assessed rigorously by that process. The same considerations apply to bulk personal datasets, bulk equipment interference and bulk interception.
53. The ability of bulk intervention will make available a wide range of information. The use of bulk personal datasets provides essential information to enable the SIAs to focus on the links between individuals who threaten national security.
54. The notion that these techniques will be used casually to obtain personal information on innocent citizens is absurd, not a reality at all. However, were any evidence of such unjustified activity to emerge, it should be subject to strong disciplinary measures and also to criminal sanctions.
55. It would be useful to receive greater clarity on the extent to which bulk equipment interference infiltrates equipment. Will it provide access to the entirety of equipment being targeted? For example, Notes for Guidance might provide greater

clarity in relation to interference with a bulk selection of smartphones - which would not just include the desired information, but also access to the entirety of information on for those phones.

56. It would be helpful if the authorisation of a warrant routinely contained an operational purpose. Information collected should complement that operational purpose.
57. Information outside the operational purpose should generally not be useable as evidence.

Oversight.

- **What are the advantages and disadvantages of the proposed creation of a single Judicial Commission to oversee the use of investigatory powers?**

58. The proposal to consolidate all commissioners who oversee all investigatory powers exercised by public authorities is welcome.
59. For the SIAs and law enforcement it is important that coordination with commissioners is effective, clear and straight-forward. A single Investigative Powers Commissioner can deliver that.
60. Consolidating the oversight of all investigative powers under one senior commissioner will require a profound knowledge of the powers, the law by which they are governed AND the security and operational climate in which the powers are enacted. The appointment and training of the judges must recognise this. All judges involved in the scrutiny of the work of the SIAs must be fully trained, including contact training with the SIAs, to understand the nature of the work that they do and the information that is required to protect the national security of the UK and the privacy of its citizens.
61. Consideration should be given to the appointment as IP Commissioner of a serving rather than retired member of the Judiciary. This implies no criticism of retired judges. In my view the perception of the importance of the role would be enhanced by the secondment of a very senior judge to the role, though continuation for a period after retirement would be acceptable.
62. It is also of high importance that the Judicial Commission does not become politicised. This is a possibility if one body oversees all investigatory powers. Selection of the Judicial Commissioners should remain independent of Government, and placed in the hands of the Lord Chief Justice for the time being.
63. A sufficient number of judicial commissioners will be needed to allow the warrantry authorisation to remain efficient and able to sufficiently cope with the number of warrants requested per year. In 2014 the warrants authorised were:
    i. 2795 interception;
    ii. 2091 property interference; together with
    iii. 321 intrusive surveillance authorisations.

Alex Carlile
Lord Carlile of Berriew CBE QC

14 December 2015

Center for Democracy & Technology—written evidence (IPB0110)

Introduction

1. The Center for Democracy & Technology ('CDT') welcomes this opportunity to submit written evidence to the Parliament of the United Kingdom's Joint Committee ('the Committee') on the Draft Investigatory Powers Bill ('Draft Bill'). CDT is a non-profit organization that works to preserve the user-controlled nature of the Internet and champion freedom of expression around the world.

Summary

2. Many of the powers in the Draft Bill are plainly incompatible with the ECHR or EU law. (¶¶ 7–18)
    a. The surveillance authorisation scheme set out in the Draft Bill is incomplete and falls short of human rights standards. (¶¶ 9–11)
    b. Legislation providing for data retention notices that could potentially require the retention of the communications data of every individual in the UK is manifestly incompatible with the rights to privacy and the protection of personal data. (¶¶ 12–14)
    c. Provisions for 'targeted' surveillance or equipment interference do not create the level of foreseeability required by the ECHR or impose legal protections sufficient to ensure that all interferences with privacy rights are strictly necessary, proportionate and non-discriminatory. (¶¶ 15–18)
    d. We make recommendations with respect to human rights law in ¶ 24.
3. The definitions in the Draft Bill are insufficiently narrowly defined. (¶¶ 25–30)
    a. We recommend that (1) definitions should be narrow, technically-grounded, and unambiguous so as to make clear the intended scope of powers and (2) updates to definitions in the statute should be: (a) approved by a vote of the Technical Advisory Board contemplated in the Draft Bill and (b) provided for by means of an affirmative Statutory Instrument, to ensure Parliamentary oversight.
4. The level of intrusiveness of IP resolution into private lives of innocent people is disproportionate, and, we believe, contravenes the ECHR and the Charter of Fundamental Rights of the European Union. (¶¶ 31–37)
    a. CDT recommends that the requirement to create and retain ICRs be struck from the bill entirely, and that targeted data preservation orders be used instead.
5. Both targeted and bulk equipment interference pose grave risks and should be narrowed substantially. (¶¶ 38–43)
    a. The standard for issuing an EI warrant should require that EI should only be used where other means are not available/feasible.
    b. Neither the police nor the security and intelligence services should have access to powers to undertake bulk equipment interference.

c. The government should clarify what conduct can and cannot be authorised in an interference warrant.

6. The Draft Bill should clarify whether the government can compel service providers to cease offering end-to-end encryption in their products and services. (¶¶ 44–48)

Are the powers compatible with the Human Rights Act and the European Convention on Human Rights ('ECHR')?

7. Many of the powers in the Draft Bill are plainly incompatible with the ECHR or EU law.

8. We recall at the outset that under Article 8 of the ECHR, *'powers of secret surveillance of citizens, characterising as they do the police state, are tolerable … only in so far as strictly necessary for safeguarding the democratic institutions.'*[216] It is our view that the exercise of surveillance powers is permissible under the Convention only where this heightened standard is met, and not merely where the collection or retention of data – or surreptitious interference with devices – would be, or could someday prove to be, convenient for the authorities. We observe that the Court of Justice of the EU ('CJEU') has adopted similar language in cases concerning data retention and surveillance.[217]

The surveillance authorisation scheme

9. **As an initial matter, the surveillance authorisation scheme set out in the Draft Bill is incomplete and falls short of human rights standards, notwithstanding the fact that it may represent some degree of improvement over the current system.** As we have pointed out in written evidence submitted to the Joint Committee on Human Rights,[218] Article 8 of the ECHR requires that all secret surveillance practices must be *'subject to effective supervision'* by the judiciary or, at minimum, a similar body that is *'independent of the authorities carrying out the surveillance'*.[219] Under the proposed scheme, however, some highly intrusive surveillance powers, such as the targeted acquisition of communications data, the issuance of data retention notices and the issuance of potentially sweeping national security notices, would not require any form of judicial or equivalent *ex ante* independent approval at all.[220]

10. Moreover, even where the exercise of surveillance powers requires the approval of a judicial commissioner, the commissioner will apply only the attenuated 'judicial review' standard.[221] We believe this form of review cannot be regarded as *'effective supervision'* for the purposes of the Convention.[222]

---

[216] *Klass and others v Germany*, [1978] ECHR 4, Judgment (Plenary), 6 Sept. 1978, ¶ 42; see also *Rotaru v Romania*, [2000] ECHR 192, Judgment (Grand Chamber), 4 May 2000, ¶ 47; *Kennedy v the United Kingdom*, [2010] ECHR 682, Judgment, 18 May 2010, ¶ 153.

[217] *Digital Rights Ireland v Minister for Communications, Marine and National Resources et al*, Judgment, [2014] EUECJ C-293/12, 8 Apr. 2014, ¶ 52; *Schrems v Data Protection Commissioner*, Judgment, [2015] EUECJ C-362/14, 6 Oct. 2015, ¶¶ 92-93.

[218] Center for Democracy & Technology, 'Written evidence submitted by the Center for Democracy & Technology to the Joint Committee on Human Rights regarding the Draft Investigatory Powers Bill', 7 Dec. 2015, https://cdt.org/files/2015/12/CDT-JCHR-written-evidence.pdf.

[219] *Rotaru*, *supra* n. 216, ¶ 59; *Klass*, *supra* n. 216, ¶ 56.

[220] Draft Investigatory Powers Bill (hereinafter 'Draft Bill'), §§ 46, 71 and 188.

[221] See, e.g., *ibid.* at § 19(2).

[222] *Rotaru*, *supra* n. 216, ¶ 59.

11. Finally, as detailed in our submission to the Joint Committee on Human Rights, we believe the appointment process and potentially indefinite renewable terms would prevent the judicial commissioners from being fully independent of the Executive – the part of government that will be responsible for conducting much of the surveillance – in violation of the ECHR's independence requirements.[223] Where the renewable nature of the commissioners' terms is concerned, we observe that by contrast, judges appointed to the Foreign Intelligence Surveillance Court in the United States serve single, non-renewable terms of no more than seven years (whilst otherwise continuing to enjoy the life tenure guaranteed to federal judges under Article III of the US Constitution).[224]

Data retention and bulk powers

12. **In our view, legislation providing for data retention notices that could potentially require the retention of the communications data of every individual in the UK is manifestly incompatible with the rights to privacy and the protection of personal data, as found in the Charter of Fundamental Rights of the European Union ('the Charter') and applied by the CJEU in its *Digital Rights Ireland* judgment.[225]** In that case, the Court invalidated the Data Retention Directive not only due to its failure to place firm strictures on access to the data, but, first and foremost, because it:

    a. *'cover[ed], in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime'*;[226]

    b. did not include exceptions for *'persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy'*;[227] and

    c. did not *'require any relationship between the data whose retention [was] provided for and a threat to public security'*: in particular, it failed to require a link, *'even an indirect or remote one'*, between the persons affected and serious crime, and further failed to place temporal or geographic limitations on the data to be retained.[228]

13. The data retention notices contemplated in the Draft Bill clearly violate EU law as these three elements from the *Digital Rights Ireland* judgment directly apply. There is also a strong likelihood that they violate Article 8 of the ECHR, which the European Court of

---

[223] See *Rotaru*, *supra* n. 216, ¶ 59; *Klass*, *supra* n. 216, ¶ 56.
[224] 50 U.S.C. § 1803(d).
[225] Charter of Fundamental Rights of the European Union, Articles 7 and 8; *Digital Rights Ireland, supra* n. 217, ¶¶ 45-69.
[226] *Digital Rights Ireland*, supra n. 217, ¶ 57; see also *Schrems*, supra n. 217, ¶ 93 (*'Legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to'* a third country *'without any differentiation, limitation or exception being made in the light of the objective pursued'*). Much of the language in this section of our submission is drawn from *Center for Democracy & Technology and Privacy International, Third-party intervention*, Conseil d'État (France), Contentious Section, N° 393099: FDN et al. c/ Gouvernement (forthcoming).
[227] *Digital Rights Ireland*, supra n. 217, ¶ 58.
[228] *Ibid.* at ¶¶ 58-59; cf. *Schrems*, *supra* n. 217, ¶ 93 (indicating that legislation concerning the storage of personal data must set out *'an objective criterion … by which to determine the limits of the access of the public authorities to the data, and of its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference'* which access to and use of the data entail).

Human Rights ('ECtHR') has previously interpreted as prohibiting a scheme under which the UK authorities, in a *'blanket and indiscriminate'* fashion, had the power to retain the biometric information of individuals who had not been convicted of a crime.[229]

14. For the same reasons, we believe the bulk powers contemplated by the bill are incompatible with EU law[230] and the ECHR at least insofar as they could be read to permit the indiscriminate and indefinite surveillance of (or equipment interference affecting) individuals for whom there is no suspicion of wrongdoing. Such powers, both separately and – especially – in the aggregate, are plainly incompatible with the very notion of a democratic society.

'Targeted' surveillance that may be discriminatory or excessive

15. Even where the surveillance or equipment interference contemplated by the Draft Bill is ostensibly 'targeted', we are gravely concerned that the relevant provisions do not create the level of foreseeability required by the ECHR or impose legal protections sufficient to ensure that all interferences with privacy rights are strictly necessary, proportionate and non-discriminatory.

16. In particular, we note that under the Draft Bill, 'targeted' interception and equipment interference warrants could relate to *'a group of persons who share a common purpose or who carry on, or may carry on, a particular activity'*.[231] We recall the ECtHR's repeated statement that any domestic law authorising secret surveillance measures *'must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures'*.[232] In our view, the Draft Bill's reference to *'a group of persons who ... carry on, or may carry on, a particular activity'* is so facially vague as to breach this aspect of the legality requirement of Article 8 of the Convention. Such language does not, by its terms, exclude the possibility that everyone who belongs to a certain trade union, political party or book club; visits a certain shop; attends (or has friends or family members who attend) a certain house of worship; subscribes to a certain publication; participates in a lawful and peaceful demonstration; celebrates or may celebrate a certain religious or national holiday; or uses a particular e-mail or instant messaging service may experience very serious privacy intrusions pursuant to a 'targeted' warrant in a manner that cannot reasonably be regarded as foreseeable. It also does not provide adequate protection against the possibility that 'group[s]' will be targeted for privacy interferences in a manner that violates the anti-discrimination provision of the ECHR (Article 14).

17. Furthermore, multiple provisions of the Draft Bill would allow the government, after obtaining a judicial commissioner's approval of a surveillance warrant, to engage in ***'any***

---

[229] *S and Marper v the United Kingdom*, Nos 30562/04 & 30566/04, Judgment (Grand Chamber), 4 December 2008.
[230] See Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, Articles 5(1) and 15(1) (requiring Member States to prohibit surveillance and storage of communications or traffic data, and mandating that any exceptions to this requirement based on national security, the prevention and prosecution of criminal offences, etc., must 'constitute[] a necessary, appropriate and proportionate measure within a democratic society').
[231] Draft Bill, *supra* n. 220, §§ 13(2) and 83.
[232] See, e.g., *Weber and Saravia v Germany*, No 54934/00, Decision, 29 June 2006, ¶ 93; *Liberty and ors v the United Kingdom*, No 58243/00, Judgment, 1 July 2008, ¶ 62; *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria*, No 62540/00, Judgment, 28 June 2007, ¶ 75.

conduct *which it is necessary to undertake in order to do what is expressly authorised or required'* by the warrant – including, for example, *'the interception of communications not described in the warrant'* (emphasis added).[233] Such provisions give rise to a serious risk that any necessity and proportionality analysis undertaken by the authority issuing the warrant, as well as any review undertaken by the judicial commissioners, will be largely illusory, and that in practice the relevant surveillance activity will far exceed what is *'strictly necessary for safeguarding the democratic institutions'* (see above).

18. Our concerns about the Draft Bill's incompatibility with the ECHR and EU law extend beyond these aspects of the text, and we would welcome opportunities to submit additional remarks.

Additional evidentiary questions

19. We provide some additional responses to questions the Committee has asked here.

Is the authorisation process appropriate?

20. No. Please see paragraphs 9–11, and 17 above, as well as our written evidence submitted to the Joint Committee on Human Rights.[234]

Do the proposed authorisation regime and safeguards for bulk data retention meet the requirements set out in the CJEU Digital Rights Ireland judgment?

21. No; see paragraphs 12–13 above.

Would the proposed Judicial Commission have sufficient powers, resources and independence to perform its role satisfactorily?

22. No. Please see paragraphs 9–11, and 17 above, as well as our written evidence submitted to the Joint Committee on Human Rights.[235]

Are the appointment and accountability arrangements for Judicial Commissioners appropriate?

23. No. Please see paragraphs 9–11 above, as well as our written evidence submitted to the Joint Committee on Human Rights.[236]

Human Rights Recommendations

24. The Committee has asked *'Are the powers compatible with the Human Rights Act and the European Convention on Human Rights ('ECHR')?'*, and our answer is clearly no. The Committee should recommend that the Draft Bill be amended to:

---

[233] Draft Bill, *supra* n. 220, §§ 12(5), 81(5), 106(5), 122(7) and 135(4).
[234] *Supra* n. 218.
[235] *Ibid.*
[236] *Ibid.*

a. Provide that judicial commissioners must be nominated and confirmed by entities that are independent of the Executive and contain strong indicia of democratic legitimacy.

b. Empower judicial commissioners to review all of the factual circumstances and legal evaluations underlying a warrant or other exercise of surveillance powers before deciding whether to approve it.

c. Extend the review and authorisation powers of the judicial commissioners to all forms of privacy interferences contemplated by the Draft Bill.

d. Provide that the terms served by judicial commissioners are strictly limited to a predetermined period of years and are not renewable.

e. Narrow all of the surveillance powers in the Draft Bill (including data retention and equipment interference) so as to prohibit effectively the indiscriminate and indefinite surveillance of individuals for whom there is no suspicion of wrongdoing.

f. Clarify the nature and scope of, and require judicial authorisation for, the national security notices contemplated by § 188 of the Draft Bill so as to mitigate the potential for abuse (e.g. the possibility that such notices will be used to evade judicial authorisation that would otherwise be required).

g. Restrict the 'targeted' surveillance powers in the Draft Bill in a manner that prevents their use for interferences that are discriminatory or excessive, and ensures that the nature and extent of the surveillance that may occur pursuant to these provisions are fully foreseeable to both the judicial commissioners and the public.

h. Generally, ensure that all interferences with privacy rights through secret surveillance measures meet the heightened standard of being strictly necessary for safeguarding democratic institutions.

Are the powers sought workable and carefully defined?

25. The Committee asks: *'Are the technological definitions accurate and meaningful? Does the Draft Bill adequately explain the types of activity that could be undertaken under these powers? Is the wording of the powers sustainable in the light of rapidly evolving technologies and user behaviours? Overall, is the Bill future-proofed as it stands?'*

26. The definitions in the Draft Bill are insufficiently narrowly defined. Definitions should be drafted to map unambiguously onto current features of Internet architecture and protocols so that communications service providers (CSPs) can understand what they will need to collect, retain and be prepared to produce with the proper legal authorisation.

27. We recognise the importance of ensuring that technological developments do not render the powers detailed in the bill ineffective. However, in our view the terminology is currently so broad that there is not only difficulty in mapping the legislative language to actual features of existing technology, but also real uncertainty created with respect to the scope of the powers sought in the Bill.

28. We would particularly like to draw the Committee's attention to the definitions of: 'equipment', 'communications data', 'Internet connection record', 'electronic protection', and 'system' (see paragraph 43, below).[237] Each of these terms – with the exception of 'Internet connection record' – have commonly-accepted technical definitions that should be used instead of the current definitions in the Draft Bill, which are so vague and expansive to hardly be definitional at all.

29. To ensure that the legislation provides for both statutory and technical clarity in addition to 'future-proofing', we recommend that (1) definitions should be narrow, technically-grounded, and unambiguous so as to make clear the intended scope of powers and (2) updates to definitions in the statute should be: (a) approved by a vote of the Technical Advisory Board contemplated in the Draft Bill and (b) provided for by means of an affirmative Statutory Instrument, to ensure Parliamentary oversight.

30. For example, the definition of the elements of an Internet connection record in the Draft Bill match only to some extent standard technical network connection logging facilities such as Netflow (a proprietary Cisco standard) and IPFIX (the non-proprietary equivalent standardized by the Internet Engineering Task Force). However, these technical connection logging standards can only collect lists of IP addresses, not web pages, for which additional information from users' Domain Name System queries must be included – which amounts to incredibly intrusive information, compromising a complete record of what people read and do online.

Data Retention

31. The Committee asks, *'Is accessing Internet Connection Records essential for the purposes of IP resolution and identifying of persons of interest? Are there alternative mechanisms? Are the proposed safeguards on accessing Internet Connection Records data appropriate?'*

32. The level of intrusiveness of IP resolution into private lives of innocent people is disproportionate, and, we believe, contravenes the ECHR and the Charter of Fundamental Rights of the European Union.

33. CDT submitted comments[238] to this effect to the House of Commons Home Affairs Committee's inquiry into the Counter-Terrorism and Security Bill last year. We would like to draw this Committee's attention to that submission and re-emphasise those concerns here.

34. The government have argued in the guidance notes that the bulk retention of Internet Connection Records is necessary to *'identify the communications service to which a device has connected'*, and that this new power is intended to *'restore capabilities that have been lost as a result of changes in the way people communicate'*.[239] Evidence from countries where the retention of ICRs has been extensively tried – such as Denmark[240] – suggests they will not be effective for these purposes.

---

[237] § 81(2) and 82(3) & (4).

[238] Center for Democracy & Technology, 'Comments on Part 3 of the draft Counter-Terrorism and Security Bill', submission to the Parliament of the United Kingdom Home Affairs Committee (15 December 2014), *available at:* https://cdt.org/files/2014/12/CDT-UK-CTS-Bill-comments-Part-3.pdf.

[239] Draft Bill Guidance notes, page 5.

[240] IT-Political Association of Denmark, 'Written evidence submitted by IT-Political Association of Denmark', submission to the Parliament of the United Kingdom Science and Technology Committee (8 December 2015), *available at:*

35. We would like direct the Committee's attention to the recent repeal of similar powers by Denmark and to the submission by Danish NGO IT-Pol to the Science and Technology Committee inquiry, which provides detailed evidence regarding the lack of efficacy of ICRs.[241]

36. Additionally, it is important to note that unlike with telephony, the line between communications content and communications data on the Internet is not clear. It is therefore inappropriate, and potentially misleading, to regard ICRs as merely being equivalent to telephone communications data, when in fact they can be even more revealing of private life, for example, effectively serving as a list of materials recently read, viewed, purchased, or otherwise interacted with online.

37. Given the level of intrusiveness, cost, and ineffectiveness of ICR data retention, CDT recommends that the requirement to create and retain ICRs be struck from the bill entirely, and that targeted data preservation orders (as described in our December 2014 comments[242]) be used instead.

Equipment Interference

38. The Committee asks, *'Should the security and intelligence services have access to powers to undertake (a) targeted and (b) bulk equipment interference? Should law enforcement also have access to such powers? Are the safeguards for such activities sufficient?'*

39. **Neither the police nor the security and intelligence services should have access to powers to undertake bulk equipment interference.** Such a power, for reasons described earlier in this submission (see paragraphs 15–18), is incompatible with EU law and the ECHR due to its disproportionate nature.

40. CDT is alarmed that the government seeks powers that would require service providers to assist in 'hacking' their own customers. The inclusion of the duty in § 101 to assist in giving effect to interference warrants would undermine UK consumers' trust in UK CSPs and damage UK CSPs' reputations internationally.

41. In addition, we are concerned that:

    a. A 'targeted' interference warrant does not actually target an individual and that a single 'targeted' warrant could end up monitoring many people. For example, §§ 83(d) & (e) allow for interference with any equipment in one or more locations without placing any restrictions on the scope of what is meant by location. Restricting it to 'premises' would narrow the notion of location here to a physical facility, but some facilities (such as data centres and Internet exchange points (IXPs)) contain thousands of pieces of equipment mediating communications between tens to hundreds of thousands of individual people.

    b. Equipment interference, as it necessarily entails 'breaking into' devices and services, could create vulnerabilities in CSPs' systems that could leave them open to hacking and exploitation by criminals, hostile governments or others. These vulnerabilities could damage the ability of CSPs to store the retained

---

http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25190.html.

[241] *Ibid.*

[242] CDT Counter-Terrorism and Security Bill Comments, *supra,* n. 238.

data securely as mandated in § 74 of the bill. Any equipment interference must be undertaken with appropriate safeguards that are designed to minimize the impact of impairing equipment and services.

c. Targeted EI represents an extreme and dangerous form of intrusion. It is paramount that it should only be used in a manner that is strictly lawful, necessary and proportionate (see above) and where other means are not feasible. We note that the Secretary of State, in deciding whether it is 'necessary' to issue an EI warrant, must consider *'whether what is sought to be achieved by the warrant could reasonably be achieved by other means,'* but the standard should instead require that EI should only be used where other means are not available/feasible. (§ 84(6))

42. The government should clarify what conduct can and cannot be authorised in an interference warrant. § 101(1) requires that a CSP that has been served with a warrant *'must take all steps for giving effect to the warrant that are notified to the relevant telecommunications provider'*. Similarly, although § 40(3) requires bulk equipment interference warrants *'describe the conduct that is authorised by the warrant'* it does not place any restrictions on the conduct that may be authorised. In particular, it may be possible for a bulk EI warrant to include a requirement for a company to assist with the creation of a 'backdoor' into their own encryption technology, an exceedingly dangerous prospect that can threaten the security of all communications mediated by that technology. We would prefer the Draft Bill clearly articulate what classes of interference are possible with an EI warrant, rather than merely providing for notice and a description of the content as a condition of the warrant to issue.

43. The definition of a 'system' should also be more clearly defined. § 81(2) and 82(3) & (4) note that a system is a relevant system if any communications or private information are held on or by means of the system. In the Australian context, similarly overbroad language has been interpreted as potentially including the entire Internet.[243]

Encryption

44. The Draft Bill should clarify whether the government can compel service providers to cease offering end-to-end encryption in their products and services.

45. Under current legislation,[244] UK authorities have the power to order users or communications service providers to decrypt communications, at least where the individual or company concerned has the encryption keys (or otherwise has the ability to decrypt the information). However, for CSPs that have secured their customers' communications using end-to-end encryption, it has been considered a reasonable response to a RIPA § 49 notice for a CSP to say that it cannot turn over encryption keys it does not possess. In these circumstances, companies would hand over the encrypted communication. The protections encryption provides are critical for private conversations to be possible in online environments. They are particularly important for

[243] Center for Democracy & Technology, Australian Privacy Foundation, New South Wales Council for Civil Liberties, and Privacy International, 'Joint Submission to the United Nations Human Rights Council Twenty-third Session of the Universal Periodic Review Working Group' (November 2015), *available at:* https://cdt.org/insight/expert-report-led-by-cdt-finds-that-australian-surveillance-violates-human-rights/.

[244] RIPA, § 49 http://www.legislation.gov.uk/ukpga/2000/23/section/49

privileged communications (e.g., Attorney-Client privilege) and sensitive finance, health, business, and critical infrastructure (power, water, public health, &c) communications.

46. The Draft Bill replaces the current obligation to maintain permanent interception capability[245] with one that requires CSPs to maintain permanent capabilities *'relating to the powers specified under the Draft Bill.'* Those capabilities, which are set out in § 189, include *'obligations relating to the removal of electronic protection applied by a relevant operator to any communications or data'*. This obligation is of particular concern.

47. The government have stated that the new legislation *'will not impose any additional requirements in relation to encryption over and above the existing obligations in RIPA.'.*[246] However, although the Draft Bill does not ban encryption, in practice it will be possible under the new bill for the Home Secretary to issue a § 198 'Technical Capability Notice' imposing obligations on CSPs which could prevent them from protecting communications through end-to-end encryption.

48. The ambiguity created by the provisions in the bill relating to encryption raises a critical question: is it the governments' intention to be able to mandate backdoors in communications by issuing notices – both domestically and to companies overseas – that would prevent the application of end-to-end encryption? Such a move would lead to a loss of confidence in UK technology companies globally and would damage investment in the broader UK technology sector. This impact would be especially pronounced for UK technology companies with overseas customers.

Conclusion

49. Thank you for the opportunity to submit written evidence on the Draft Bill. If we can be of further assistance, please do not hesitate to contact us.

21 December 2015

[245] RIPA, § 12 http://www.legislation.gov.uk/ukpga/2000/23/section/12
[246] Draft Bill Guidance notes, page 29.

Martin Chamberlain QC—supplementary written evidence (IPB0133)

1. Do the oversight mechanisms in the draft Bill satisfy the requirements of Article 8 of the European Convention on Human Rights?

It is regrettably impossible to give a helpful answer to this question either in the time available or, probably, at all. The following points may, however, be made:

i. The question whether **existing** oversight mechanisms satisfy Article 8 standards is itself currently before the European Court of Human Rights. The outcome of that litigation may not be known before this Bill is enacted. It is likely to be highly material to the question whether the safeguards in the Bill are compliant with Article 8.

ii. In any event, the question whether the oversight arrangements are Article 8 compliant will depend on an analysis of the whole statutory regime, including any Codes of Practice and an understanding of the way in which that regime is implemented in practice. Parliament's aim at this stage should be to make the statutory safeguards as robust as possible so as to give the Bill the best chance of being held compatible with Article 8.

iii. Some of the points highlighted below could be relied upon individually or cumulatively in support of an argument that the oversight regime does not comply with Article 8. Addressing and remedying them would make such an argument less likely to succeed.

2. What is the legal status of the Codes of Practice under RIPA? What do you expect to be contained in the Codes of Practice issued under this Bill?

i. Under s. 71 of RIPA, the Secretary of State is obliged to issue one or more Codes of Practice relating to the exercise and performance of the powers and duties imposed under Parts I to III of RIPA, s. 5 of the Intelligence Services Act 1994 and Part III of the Police Act 1997. By s. 72(1), a person exercising or performing any power or duty in relation to which provision is made by a Code of Practice must, in doing so, have regard to the applicable provisions of the Code. By s. 72(4), courts, the IPT, and Commissioners must take the Codes into account when determining any question to which they are relevant.

ii. Some limited insight as to as to the expected contents of the Codes published under the provisions in the Bill can be obtained from Sch. 6, paragraphs 2(2), 3(2) and 4(1).

iii. It is to be welcomed that Codes prepared under the Bill are in principle subject to Parliamentary scrutiny and must be approved by a resolution of each House of Parliament (Sch. 6, paragraph 5(4)). **It may, however, be noted that, once made, Codes approved in this way can be revised by the Secretary of State, apparently without the approval of either House and without any opportunity for either House to annul the Code. (Sch. 6, paragraph 6(2) & (3) require consultation in relation to any proposed revision, but paragraph 6(5) & (6) require only that the regulations effecting**

the revision, and the revised Codes, be laid before Parliament. This appears to be the only statutory instrument making power in the Act that is not subject, at least, to annulment pursuant to a resolution of the House of Commons: see cl. 197.)

iv. This is of particular significance given that certain important safeguards, including those relating to legal professional privilege and journalists' sources, are entirely absent from the Bill itself and are instead to be dealt with in the Codes (see Sch. 6, paragraph 4(1)). It is a matter of some concern that the Secretary of State could in principle remove or modify these important safeguards without any need to secure the consent of either House of Parliament and without any power in either House to annul the regulations giving effect to the removal or modification.

3. What practical effect is the introduction of a right of appeal from the Investigatory Powers Tribunal likely to have?

i. At present, there is no right of appeal from decision of the IPT. It has yet to be resolved whether the IPT is subject to judicial review under the principles in *R (Cart) v Upper Tribunal* [2012] 1 AC 663. The Government has in the past taken the view that it is not. This would be problematic even if (as was probably envisaged with RIPA was enacted) the IPT's case-load involved mainly questions of fact (eg whether this or that warrant complied with the statutory requirements and was proportionate), because even specialist tribunals sometime make mistakes. But the IPT does not deal only with questions of fact. As its recent rulings in the *Liberty* and *Belhaj* cases show, its functions include determining important and significant points of law, such as the compatibility with Article 8 ECHR of the domestic interception regime. It is highly anomalous that questions of this sort – which are likely to found applications to the European Court of Human Rights – should be finally determined by a first instance tribunal, even a specialist one such as the IPT, with no possibility of domestic appeal.

ii. It may be noted that the right of appeal conferred by cl. 180(1) is limited. Not only must leave be given by the IPT or the appeal court, but leave can be given only where (a) the appeal would raise an important point of principle or (b) there is another compelling reason for granting leave (see the new section 67A(4), to be inserted into RIPA). This restrictive test is modelled on the test for **second** appeals in rule 52.13(2) of the Civil Procedure Rules 1998. But this is a **first** appeal. It is unclear why such a restrictive test is considered necessary here. There is no similar restriction on appeal from the Special Immigration Appeals Commission (see s. 7 of the SIAC Act 1997, which confers a right of appeal "on any question of law material to [the] determination").

iii. Subject to that, the creation of a right of appeal is to be welcomed. It will bring the IPT into the mainstream of the justice system and enable significant points of law to be considered by the appellate courts in England & Wales and Scotland, and ultimately by the Supreme Court

4. Why is it important that the Investigatory Powers Tribunal is able to hold as much of its proceedings in public as possible?

i. The IPT has long recognised the importance of holding as much as possible of its proceedings in open. In its *Kennedy* ruling in 2003, the IPT held that parts of its own procedural rules were *ultra vires* and so must be disapplied insofar as they prevented it from holding oral hearings in public and giving reasoned open determinations on questions of law. In the light of this ruling the IPT has held a number of open hearings to determine points of law on assumed or hypothetical facts. In 2015, it is understood that the IPT held as many as 23 days of open hearings.

ii. As a result of some of these recent hearings, information has been disclosed about the policies and practices of the intelligence agencies that has previously not been known. However, to date this disclosure has always been with the consent of the intelligence agencies. The IPT has not to date held that it has power to require the agencies to disclose publicly material which they do not wish to disclose. This means that, in practice, the intelligence agencies themselves decide what can and cannot be disclosed. The only exception is the fact of an IPT determination, which the IPT is required by s. 68(4) of RIPA to make known to the complainant even if the agencies consider that it would be damaging to national security to do so.

iii. It would add to the credibility of the IPT as an oversight mechanism, and to its ability to contribute to compliance with Article 8 standards, if it were given express power to decide for itself whether material deployed before it should be made public and to what extent. In exercising this power, it would of course consider carefully any arguments made to it by the agencies that disclosure would be damaging to national security or another protected public interest, but it would ultimately have the function of deciding that question for itself. It should also have the power to balance any damage caused by disclosure to national security or other protected public interest against the public interest in transparency.

5. Is it appropriate that material acquired from targeted equipment interference warrants may be used as evidence in legal proceedings? Is it desirable?

It is both appropriate and desirable, subject to safeguards for special categories of material (legal professional privilege, journalists' sources etc.).

6. Is there an on-going justification for intercept material remaining inadmissible in legal proceedings?

No. The Government's long-standing opposition to any relaxation of the prohibition on admitting intercept evidence in legal proceedings (apart from in closed material procedures) is invariably based on security objections form the intelligence agencies. These objections are not compelling given that intercept material is admissible in other common law jurisdictions that place a high value on national security, such as the United States, where intercept is frequently relied upon in terrorism and other serious criminal trials.

7. The Bill creates a new offence of disclosing the fact that warrants for equipment interference have been authorised and that such activities have taken place (Clause 102). Will this have any impact on legal proceedings in your view?

The absence from Part 5 of the Bill (Equipment interference) of any provision equivalent to cl. 42 (which makes intercept inadmissible in legal proceedings) may indicate that it is intended that the product of equipment interference should in principle be admissible. If that is the intention, it should perhaps be made clear that a person disclosing the fact or product of equipment interference for the purpose of court proceedings would not commit the offence in cl. 102. Otherwise, there is a danger that a court might read cl. 102 as preventing it from ordering disclosure or, or receiving evidence as to, these matters.

8. Is the retention of data for 12 months a proportionate balance between the needs of the security services and law enforcement and the rights of the individual?

I do not know enough about the technical needs and capabilities of the intelligence agencies to answer this question confidently.

9. Does clause 13(2) meet common law and ECHR requirements as to the detail to be included in warrants and is it sufficiently clear in its terms, for example in explaining what is meant by group etc. or does it require significant amendment if it is to remain in the Bill?

I have read in draft the answer given to this question by Matthew Ryder QC. I agree with it and have nothing further to add. As to the standards required under Article 8 ECHR, the recent decision of the Grand Chamber of the European Court of Human Rights in *Zakharov v Russia* (Application No. 47143/06), Judgment 4 December 2015, suggests at §264 that targeted interception authorisations must clearly identify either a specific person or a specific set of premises.

10. Should the present powers relating to bulk interception warrants be replicated in the draft Bill or should warrants be more narrowly focused as to their purpose and permitted search criteria?

It is regrettably impossible to give a helpful answer to this question in the time available.

11. Are the proposals in the Draft Bill at s. 89 and following adequate to deal with the range of intrusions that are possible? Are you concerned about the current lack of an associated draft Code of Practice?

It is regrettably impossible to give a helpful answer to this question in the time available.

12. Section 102 creates an offence of unauthorised disclosure of equipment interference warrants. What impact could this have to the disclosure obligations under the Criminal Procedure and Investigations Act 1996? What is your opinion of the hypothesis that defendants will routinely allege hostile equipment interference on their computers and smart phones by law enforcement and that defence lawyers will then seek to have such evidence excluded for unreliability and potential contamination under s 78 PACE?

It is regrettably impossible to give a helpful answer to this question in the time available.

22 December 2015

Chartered Institute of Legal Executives—written evidence (IPB0041)

1. Introduction

1.1 The Chartered Institute of Legal Executives (CILEx) welcomes the intention to consolidate the complex area of law surrounding the use of investigatory and surveillance powers.

1.2 A simplified and consistent framework for the use of these powers is necessary to balance the needs for privacy and civil liberties with the need for protection and public safety.

1.3 It is equally important that the rules are transparent for the public to have confidence in how the powers are used.

1.4 This written evidence relates in the most part to judicial authorisation, and confidential communications between a client and their lawyer; commonly called 'legal professional privilege.'

2. Chartered Legal Executives

2.1 CILEx is an Approved Regulator under the Legal Services Act 2007, and the professional association for Chartered Legal Executive lawyers, paralegals, and other legal professionals in England and Wales. We have around 20,000 members, including more than 7,500 fully qualified lawyers known as Chartered Legal Executives.

2.2 Chartered Legal Executives are specialist lawyers. They are Authorised Persons under the Legal Services Act 2007, with automatic rights to act as Commissioners for Oaths, and can be authorised for independent practise in litigation, advocacy, probate, conveyancing and immigration, depending on their specialism. They work in all areas of law, in private firms, local authorities, charities, and for government departments. They can set up their own law firms, become partners in established firms, and are eligible for judicial appointments.

2.3 The majority of Chartered Legal Executives studied through a vocational or apprenticeship-style route to qualify. Because it is a more accessible and affordable route to a legal career, three-quarters of CILEx lawyers are women, and a third of new students are from Black, Asian or Minority Ethnic backgrounds.

2.4 In recent years CILEx lawyers have increased their opportunities to practise law independently, giving them parity with other types of lawyers. These changes, approved by Parliament[247], are important for diversifying the legal profession, encouraging new businesses, and expanding choice for consumers.

2.5 CILEx Regulation Ltd independently regulates CILEx members and entities in the public interest. They are currently consulting on applications for powers to license Alternative Business Structures (ABSs), which will further expand consumer choice.

2.6 The Draft Bill under consideration will likely impact on legal professional privilege, which applies to the communications between Chartered Legal Executive lawyers and their clients. It is important that any laws impacting on the legal profession or justice system recognise the complete range of lawyers providing services to the

[247] http://www.cilex.org.uk/media/media_releases/new_practice_rights_approved.aspx

public to ensure the law is fit for purpose and does not require subsequent time-consuming revisions.

3. Scope of legal professional privilege (LPP)

3.1 Communications between a client and their Chartered Legal Executive are subject to LPP, in the way same as between a client and their solicitor or barrister.

3.2 This was made explicit by the UK Supreme Court in a 2013 judgment[248] clarifying the extent of legal advice privilege.

3.2.1 Legal advice privilege (LAP) specifically relates to the communications between lawyers and client, and falls within the wider umbrella of LPP.

3.2.2 The case centred on whether LAP should be extended so as to apply to legal advice given by someone other than a member of the legal profession (in this case to accountants advising on tax law).

3.2.3 The judgment states;

"…it is universally believed that LAP only applies to communications in connection with advice given by members of the legal profession, which, in modern English and Welsh terms, includes members of the Bar, the Law Society, and the Chartered Institute of Legal Executives (CILEX) (and, by extension, foreign lawyers). That is plain from a number of sources, which speak with a consistent voice."

3.3 It is important therefore that any provisions within the Draft Bill, or recommendations from the committee, should be consistent when referring to the professionals who have duties under LPP. It is essential that where reference is made to barristers and solicitors, there should be explicit inclusion of Chartered Legal Executives.

4. Provisions for legal professional privilege

4.1 It is important to remember that LPP is not a protection for lawyers, but for the public. It is their right to communicate with a lawyer in confidence, and not have those communications intercepted.

4.2 As stated above, CILEx welcomes the moves to consolidate this complex area of law. However the Draft Bill may potentially miss the opportunity to protect the confidentiality of communications which should be subject to LPP.

4.3 Lawyers are under a duty to keep their communications with their clients confidential. This is essential for the proper administration of justice, with the public holding a fundamental understanding that their communications with their lawyer are confidential.

4.4 Instruments of the State and the legal profession have joint responsibility to uphold this public trust. If this is undermined, it could jeopardise the nature and content of these communications, which will impede a lawyer's ability to properly advise their clients based on all the information.

[248] *R (on the application of Prudential Plc and another (Appellants)) v Special Commissioner of Income Tax and another (Respondents) [2013] UKSC 1*

4.5 The committee can be reassured that LPP is not an absolute right. It does not apply where there is reasonable suspicion that the communication is in furtherance of a criminal purpose, known as the 'iniquity exception'.[249]
4.6 In light of the above, legal professional privilege should be given statutory protection in the Draft Bill.
4.7 CILEx believes that it will not be sufficient to rely on a code of practice for this protection to be maintained in the long term, as it will have less legal force and be more easily amended.

5. Judicial authorisation

5.1 The proposed two stage authorisation process, whereby the Secretary of State and a Judicial Commissioner jointly approve a warrant, may require additional safeguards.
5.2 The purpose of the authorisation process is to independently assess the warrant application and either approve or deny on its merits and legality. The assessment of the warrant application cannot be independently made by the body submitting the warrant. The Draft Bill however allows for warrants to be enacted in 'urgent cases' without the prior approval of a Judicial Commissioner. This may be in a significant number of cases given the nature of the warrants under consideration.
5.3 CILEx believes that explicit judicial authorisation should be obtained in all circumstances. This has the advantage of warrants being independently assessed for their merits and legality, but also with judicial authorisation the evidence that is subsequently obtained is more likely to be adduced and accepted in serious cases.
5.4 Without judicial authorisation, evidence is more likely to be challenged, and dismissed on technicalities.
5.5 In matters of national security and personal freedoms, judicial approval of all intercept warrants as recommended by David Anderson QC, is both achievable and necessary.
5.6 Whatever test the Judicial Commissioner applies in authorising a warrant, it should primarily be to assess the merits and legality of the application.

6. Recommendations to the committee

6.1 CILEx requests that the committee consider the following recommendations:
- 6.1.1 The Bill should grant statutory protection of legal professional privilege, through explicitly including it on the face of the Bill. Such protection would provide reassurance to the public of the importance and preservation of this fundamental right.
- 6.1.2 If this is not to occur, then as an absolute minimum, the relevant codes referred to in the Draft Bill should be enforceable by law, and be drawn up in consultation with the legal professions.

[249] Longmore LJ in *Kuwait Airways Corpn v Iraqi Airways Co* (No 6) [2005] 1 WLR 2734

6.1.3 Any provisions made by the Draft Bill with regard to legal professional privilege should accurately reflect all the professionals on whom duties are imposed.

6.1.4 All warrants should be subject to judicial approval.

18 December 2015

Chartered Institute of Library and Information Professionals (CILIP)—written evidence (IPB0104)

Chartered Institute of Library and Information Professionals (CILIP)

1. CILIP is the professional body representing 13,000 librarians and knowledge and information managers within the UK. They work in all parts of the British economy including Government, health and social care, higher education and research, colleges and schools, industry and commerce, the third sector and public libraries.

2. The proposals in the Investigatory Powers Bill are of especial interest to our professional community in that they touch on the ethical principles underpinning good information management as well as the practical management of information resources. They go to the heart not only of trust and confidence the citizen has in Government but will also impact on the trust users and potential users have in library and information services and the integrity with which those services are provided. Our members are bound by a set of Ethical Principles and Code of Professional Practice[250] that includes "respect for confidentiality and privacy in dealing with information users". We also have a duty under the terms of our Royal Charter[251] to "scrutinise any legislation affecting the provision of library and information services",

Introduction

3. CILIP welcomes the opportunity to comment on the Draft Investigatory Powers Bill. It acknowledges the development in the Government's thinking on the balance needed to be struck between the important principles of national security and the protection of citizens and their right to privacy and freedom of thought and expression. It also appreciates the greater transparency around issues of interception, surveillance and retention of communications data and especially welcomes the publication of the Transparency Report 2015[252] and the Government's commitment to make this an annual report. We note too that members of the intelligence community have been allowed to contribute to the public debate.

4. We are concerned, however, at the speed of the consultation process over the draft Bill. This is a major topic and needs greater time for proper reflection, research and public debate on the provisions of the Investigatory Powers Bill. The three weeks allowed for contributing evidence to the Joint Committee is simply inadequate.

[250] CILIP, 2012. *Ethical principles for library and information professionals*. Revised edition. [PDF]. CILIP. Available at: http://www.cilip.org.uk/about/ethics/ethical-principles [Accessed 18 December 2015]
[251] CILIP. *CILIP Royal Charter*. Revised ed. [PDF]. CILIP. Available at: http://www.cilip.org.uk/sites/default/files/documents/CILIP%20Royal%20Charter%20-%20approved%20November%202014.pdf [Accessed 18 December 2015].
[252] Home Office, 2015. HM Government transparency report 2015: disruptive and investigatory powers. (Cm 9151) [PDF]. London: HMSO. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473603/51973_Cm_9151_Transparency_Accessible.pdf [Accessed 18 December 2015]

5. Similarly the opportunities to comment seem not to have been gathered into one place and the related Inquiries being undertaken by the Science and Technology Committee and the Joint Committee on Human Rights not sufficiently cross-referenced.

6. As a result our comments are not as full or considered as we would have wished on such an important topic. However we trust that our concerns will be considered and hopefully addressed through improved provisions within the Bill.

Overarching/Thematic Questions

Are the powers sought necessary?

7. CILIP accepts that the police, security and intelligence services need the tools to be effective in an information age and to protect the public from serious crime (including child exploitation), cyber attacks, or terrorist activity. It notes that, in most respects, this is a consolidation bill and usefully brings together provisions from a number of preceding acts. Our main concerns are:

    a. The balance between necessary and proportionate interception and surveillance and the individual right to freedom of access to information, freedom of expression, and privacy which the UK has signed up to through the UN Declaration of Human Rights and the European Convention on Human Rights - rights which underpin the provision of libraries, and
    b. The adequacy of the proposed authorisation and overview provisions.

Are the powers workable and carefully defined

8. We are concerned at what will constitute a "Communications Service Provider". Previous legislation has been restricted to public telecommunications services but it would appear that under the provisions of this Bill to include private telecommunications services, including networks operated within universities, colleges, schools and local authorities (which provide, in the main, public library networks). Neither the likelihood, feasibility or costs of this are known. It is an area we would have liked to explore further with our members as this could include the obligation to collect communications data and the use of tools such as VPN tunnelling, and so impact on the trust users of libraries would have in their library service.

Are the powers sought sufficiently supervised

9. This is our major area of concern. Although generally we accept the need for interception and surveillance to protect the public from serious crime (including child exploitation), cyber attacks or terrorist activity, it becomes very important that these powers should only be used when necessary and proportionate to achieve that purpose. In our view judicial authorisation and oversight is essential and should include applications to look at communications data as well as requests for interception. We note that under existing proposals the Secretary of State will determine whether an application is justified with the Judiciary restricted to ruling on whether the right procedures have been followed. We strongly believe that prior judicial authorisation (looking at the substance of the case being made for using the powers as well as whether the correct processes have been followed) should be required for all intrusive powers provided in the Bill. This may or may not be part of a "double-lock" procedure

as currently proposed in the Bill. We understand that prior judicial sign off is required in many other democratic countries including the Five Eyes Alliance of the USA, Canada, Australia, and New Zealand (with the UK as the other member).

Specific Questions

Communications Data

10. We share the concern of many about the security of the communications data databases that would be created and the fact that they would be obvious targets for hackers,

11. Our main concern is to ensure that there is prior judicial authorisation for all requests to access such data (see our response to question: Are the powers sought sufficiently supervised). Existing proposals for access to be authorised by senior officers of the police or security agency concerned are not adequate. We would also welcome clarification as to why storage of communications data for up to a year is felt to be justified or proportionate to the risks involved when we understand other nations specify shorter periods.

12. Such measures will be important in reassuring citizens that their data will not be irresponsibly used. It will build the trust of the citizen that the Government is acting in their best interest, and the user of the library and information service that their personal data is being treated with respect and confidentiality, It is also important that all users of the internet are apprised that such data is being collected prior to using the internet. This should be an educative function of library services of all types and form part of their information literacy programmes enabling users to become effective and knowledgeable users of information.

Data retention (Internet Connection Records)

13. We note in passing the comments of other experts about the investment required to be able to collect ICRs (internet Connection Records) as set out in the Bill and store them for up to a year. We would want at least the same judicial authorisation as we suggest for more general communications data (see our response on communications data). However our understanding is that ICRs are more intrusive than general communications data and are needed to identify the actual sender of an online communication. This is an area we would have liked to discuss more fully within our professional community.

Bulk Personal Data

14. Although not specifically given as an example in the literature we expect that library and information service records (eg library membership, loans data, reservations etc) would fall within this category. Therefore, as stated previously, we would want prior judicial authorisation as a minimum requirement.

Conclusion

15. CILIP is a member of The International Federation of Library Associations and Institutions (IFLA) that has recently issued a statement on Privacy in the Library Environment253. It notes that excessive surveillance and data collection will alter user behaviour, potentially narrowing their right to freedom of speech and freedom of expression. This illustrates both the delicacy of the information ecosystem and its global nature. CILIP, as IFLA, have supported the "International Principles on the Application of Human Rights to Communications Surveillance"254 which we feel sets out a robust framework for evaluating the powers included in legislation like the Investigatory Powers Bill.

16. We note too that the Science and Technology Committee is currently undertaking an Inquiry into Digital Skills. In responding to previous inquiries on this topic we have stressed the importance of the "I" word in IT. Skilled information managers are needed to help harness and exploit the data and information sources now available and when members of a professional body such as CILIP, they will also act within a professional ethical framework. As well as the legal framework being set up by the Investigatory Powers Bill, the skills and integrity of professional information managers will be vital to both sides of the equation – the responsible use of the data obtained by the security and intelligence community, and the proper information governance (including the education of users) by information professionals working across all sectors and including public libraries.

17. We will be happy to expand on these points if required

CILIP

December 2015

21 December 2015

253 International Federation of Library Associations and Institutions [IFLA], 2015. *IFLA statement on privacy in the library environment*. [PDF]. IFLA. Available at: http://www.ifla.org/files/assets/hq/news/documents/ifla-statement-on-privacy-in-the-library-environment.pdf {Accessed 18 December 2015]

254 Electronic Frontier Foundation (and others). 2014. *International principles on the application of human rights to communications surveillance*. [online]. Electronic Frontier Foundation (and others). Available at: https://en.necessaryandproportionate.org/text [Accessed 18 December 2015]

Tom Chiverton—written evidence (IPB0023)

1. Privacy and security are not two mutually exclusive extremes. Strong security is required for privacy, and privacy is very important for many groups, from domestic violence suffers who require privacy at home when talking to help services to those who fear persecution in their home countries.

2. While it is good that the IP bill does not contain an outright ban on encryption, what it does contain is a series of un-contestable secret warrants to force companies and individuals to decrypt en-mass.

3. This is because secure encryption can't be broken on a per-user basis. It may even be the case that 'zero-knowledge' systems are used so that this is by design impossible, or reuse open source software or online services which provides a secure encryption service.

4. Zero knowledge encryptions are typically used for the most sensitive and personal data. These are the places you would least like companies to be forced to secretly decrypt the data with out being able to explain to their users that this was happening.

5. Open source software can not easily be changed to defeat it's encryption. The unmodified software will be freely available online, and users who value privacy (or are plotting the next 'terrorist outrage') will simply use the original versions.

6. The Bill should therefore not seek to create secret back doors.

7. Being forced to make a system less secure for everyone, so that one 'person of interest' can be followed is not a good trade off between the privacy of everyone else and their security.

8. A system of open warrants, put before a judge in advance of execution, for a narrow purpose and time range, would be better.

9. The vast cost of storage and security of this decrypted data introduces significant risk to companies. Everyone from bored teenagers to foreign governments will be targeting the now less secure than it could be databases.

10. No provision is to assist private enterprises (which could be of any size) with these risks and costs.

16 December 2015

Howard Clark—written evidence (IPB0070)

1. Are the powers sought necessary?

I have to distinguish between bulk collection and specific collection and intercept. Specific collection and intercept when based upon intelligence, and with a warrant are acceptable. It is the bulk surveillance, and communications intercept that are unacceptable.

The powers sought are not necessary in my opinion for the following reasons:

1.2 Purpose:

Anti-terror legislation must have a clear purpose to ensure that the achievement of their aims can be monitored. So far there has been no evidence that Intelligence powers have described clearly what their purpose is.

In my opinion the purpose must be twofold, on the one hand yes, **'to keep the public safe'.**

But a secondary purpose must also create a balance, that of **'protect liberal democracy'.**

Purpose:

'To keep the public safe and protect liberal democracy'

The current proposals (actually trying to make law something already carried out illegally) have promoted the former, at huge risk to the latter half of their purpose.

The very act of hoovering-up huge amounts of communications and Internet data (and databases, and public vehicle movements and NHS data, and yes websites visited) undermines the two key planks required for a healthy liberal democracy. Namely a right to a private life and the right to exercise free speech.

None of this data has been consented to being shared with others.

The website data for example, goes beyond accessing phone records; it is a minute-by-minute insight into huge swathes of the populations' thinking. Data and information they do no share with even their closest loved ones or family members. It gives clues to their politics, sexuality, worries, fears and much more. The impact of such collection will have a negative impact upon the exercise of free speech and of privacy within the United Kingdom. Dangerously government and the police would have more access to information about individuals than any time in history. All without their consent. This changes the nature of the United Kingdom's liberal democracy to a surveillance state. The unintended consequences for our democracy are far-reaching.

1.3 Consent

So far the arguments presented to support the powers in this bill have been unconvincing.

For example, the argument that Tescos has more knowledge about its customers than the police or intelligence services do. There is a fundamental difference here of purpose here. On the one hand I don't care if Tescos knows I buy Baked Beans (although I certainly don't myself share this information with them).

Secondly, it is my choice if I decide to consent to do so in exchange for some form of benefit. Personally I would like to see more controls and limitations that all companies gather and share.

1.4 Trust … and prosecutions for breaking the law in the first instance

Thirdly, why should these powers be handed to an intelligence or police service that introduced many of these surveillance practices without recourse to parliament or the public in the first place? Where are the criminal prosecutions and investigations into how and why these huge infringements on civil liberties and liberal democracy were allowed to happen in the first place?

1.5 The use of surveys - The Public don't mind it

In David Anderson's report, A Question of Trust, he cited a number of surveys and suggested that these showed the British public didn't mind the surveillance.

Each of the surveys is of very small samples, carried out mostly by newspapers and some opinion polls. At least one of these warned that it's figures should not be used or cited as there were methodological problems with them. Often the surveillance issue is 1 question, parceled in amongst lots of others. At other times, the survey data actually related to a specialist panel and not to an open opinion poll. At other times, there are not enough details about survey methodology to seriously critique them. These do not justify David Anderson's conclusions. Perhaps Anderson's specialism is the law, and he should never have strayed into territory he is not really equipped to make judgments upon?

I for one, and after speaking to many of my friends really DO mind these surveillance powers and we believe they seriously undermine the nature of our democracy. The best response to terrorism is not to do the work of the terrorists, but to *strengthen* the rights and privileges.

1.6 The timescales & nature of the review

I do apologise that this is somewhat poorly written. I would have taken longer but there was little time given to prepare. And this is another concern.

Instead of including a broad debate across society, including academics and the public, this has been reviewed by the legal profession to the exclusion of many others who also have an interest in and concern for liberal democracy and civil society. I have profound worries for the unintended consequences that this bill will have upon the United Kingdom and her standing in the world. Worries that are not addressed by judicial oversight or Home Secretary sign-off, of mass surveillance proposals such as these.

And since this is supposedly about trust, allowing such a short period to respond and properly examine these proposals undermines my sense of trust.

1.7 Big Data … unintended consequences

Treating the public as populations to be milked for bulk data and communications in this way, puts us into the realm of more oppressive regimes. Worse it has an impact upon how the British are viewed around the world, an impact upon trade and tourism etc.

Another point is how it changes the British public from people electing Members of Parliament to represent their views, to data sets to be monitored and squeezed and sifted for information. The state becomes ' a hollowed-out 'panopticon' democracy, instead of a rich liberal parliamentary democracy.

However, from my understanding is that the current failures that have led to attacks were caused by intelligence failures. Not from the lack of bulk collection of communications and data.

One unintended consequence could see people who would normally share worries or concerns with the authorities as less likely to come forwards if their views of the intelligence services (and of government) change to a more hostile view. This is, I think one impact of mass surveillance societies. They are incompatible with the proper functioning of liberal democracy.

2.0 Are the powers sought legal?

No, they are not compatible with the HRA or the ECHR.

The proportionality that they only are exercised when necessary is lost in the act of gathering the data in the first place (back to the purpose above).

Yes I am worried about accessing journalist's communications, but I am also concerned about accessing everybody else's communications. Other people have privileged communications. But these are not just phone calls, these are medical records, and everything else. The powers in this bill give access to what people are thinking. I am truly shocked that this is even considered proportionate.

2.1 Extending truly shocking powers to a broad range of state players

Just too appalling for words. The idea that this oppressive surveillance regime then moves into the hands of the broader public bodies is piling bad ideas on top of bad ideas.

3.0 Are the powers sought workable and carefully defined?

No.

I am not technically minded, I leave that to others. However, even if these things could be done, this focus firstly must be *should* they be done? What are the unintended consequences?

4.0 Are the powers sought sufficiently supervised?

No. With this level of intrusion into privacy, and he unintended consequences on free speech, only double-lock permissions should be available. The Secretary of State is too close to a conflict of interest and if judges do have the right to sign-off, there must extra protections in place.

21 December 2015

Dr Richard Clayton—written evidence (IPB0085)

In late November I submitted detailed technical evidence to the Commons Science & Technology Select Committee Inquiry regarding the technical detail of Internet Connection Records (ICRs), so I will not repeat that here. In this submission I build on that evidence to draw your attention to the technical failings of what is proposed and some of the wider policy issues surrounding ICRs.

1. I am the Director of the Cambridge Cloud Cybercrime Centre based in the Computer Laboratory of the University of Cambridge. I have a particular interest in how it is possible to trace people who are communicating over the Internet and I am one of the leading academic experts on how this can be done (and what might go wrong in practice).
2. To avoid unnecessary repetition, this evidence assumes a familiarity with the explanations I provided in my evidence to the Commons Science & Technology Select Committee, which has been published by them at:

   http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25145.pdf
3. Although ICRs are apparently discussed at length in the Draft Bill there is in fact no actual detail as to what they might comprise. I (and many others) assume that what is intended is that (non-sampled) Netflow data will be collected, details such as the number of bytes transferred will be redacted and all this data will be stored for a year.
4. This will require the deployment of new (and expensive) equipment at many, if not all, of the major Internet access providers and will require the creation of very substantial (and expensive) databases of personal data about the activities of the population of the UK ‘just in case’ this data might be useful.

Traceability

5. It is clearly intended that ICRs will address the current traceability problem with mobile networks because, in their ‘Carrier Grade NAT’ systems, a single IP address is shared by many hundreds of different people.

6. Law Enforcement piously hopes that by performing 'intersection attacks' (correlating multiple events and tracing back the IP addresses) they will find that only one person is a member of the multiple groups of "many hundreds".
7. Unfortunately, this may not be the case in practice if Internet access providers have engineered their systems to efficiently record data under the existing DRIP Act regime. They will have static IP address allocations for each user (see RFC7422 for a discussion) and so every group of "many hundred" people will contain the same "many hundred" and the intersection attack will be entirely ineffective.

New functionality

8. The Draft Bill requires ICRs to be recorded by all Internet access providers, not just the mobile companies who are using Carrier Grade NAT. Traceability alone does not justify this requirement. Instead, Law Enforcement is seeking brand new capabilities.
9. The Draft Bill sets out three ways in which ICRs can be lawfully used; #1 to identify a specific user of a service (as I have just discussed); #2 to identify what services someone uses; and, #3 to identify who is making use of a service.
10. Rapid identification of the services someone uses (#2) is a new capability – previously only achievable by performing an interception or by forensic examination of a seized computer. The list of IP addresses (and port numbers) can be interpreted to give a list of websites visited, mobile apps in use and hence hobbies, interests and concerns. This type of data clearly involves a very significant intrusion into peoples' lives.
11. I think it is unacceptable that this new power is authorised in exactly the same manner as what is essentially just a reverse directory lookup – a strong case can be made that it should be authorised at the same (very high) level as an interception.
12. Identifying who is making use of a service (#3) is also a new capability – and it was previously only achievable either with the co-operation (or seizing) of the service (so that logs could be inspected) or by interception of traffic to the service. The new capability will allow rapid stereotyping of individuals (for example, 'list everyone who has visited www.conservativehome.com') with none of the checks and balances inherent in the current methods of obtaining mass surveillance data.
13. Once again I am very surprised to see that this very significant capability can be wielded by a Superintendent without at the very least requiring permission from the judiciary.
14. However, there may be a significant gap between what the #2 and #3 provisions promise to deliver and how it works out in practice. There is an inherent assumption here that there is a one-to-one correspondence between an ICR and an intentional visit to a website and that is not the case today and will be far less so in the future.
15. Some modern browsers 'prefetch' data so that when you click on a link the page will be immediately available. In these circumstances, ICR will record a 'visit' to a linked website whether the link is clicked or not.
16. Modern websites can be extremely complex with text, images and adverts being served from dozens of different servers. The ICR data will be unable to distinguish between a visit to a jihadist website and visiting a blog where, unbeknown to the visitor (and the

blog owner) the 329th comment (of 917) on the current article contains an image which is served by that jihadist site.

17. So an ICR will never be evidence of intent – it merely records that some data has flowed over the Internet and so it is seldom going to be 'evidence' rather than just 'intelligence'.
18. There is no public evidence for the efficacy of using ICR data for purposes #2 and #3 (how often the results are actually of use compared with how often there are 'false positives'). Given the huge costs incurred in creating these systems I believe that every taxpayer would wish to see a favourable cost/benefit analysis.
19. I hesitate to say that there is no evidence here at all because the agencies have the experience of operating the mass surveillance systems revealed by Edward Snowden – the Inquiry might usefully ask what this cost/benefit analysis currently shows.
20. However, there is a real difference in deploying a monitoring technique in secret and a future world in which the Bad Guys know of the monitoring and are trying to hide their signal in the noise. I expect to see deliberate 'chaffing' (creating ICRs of spurious visits to large numbers of irrelevant websites) to obscure the visits that matter (modern malware already does this to try and make it harder to identify command-and-control sites).
21. I also expect to see widespread 'smearing' of innocents by tricks such as the comment image I have just described. The bottom line is that countermeasures will be taken against this new tracking technology and those countermeasures will make it far less effective than today – and by creating considerably more ICR data they will most likely raise its cost by an order of magnitude.

The filter

22. Clearly, when processing ICRs there is a need to process a lot of data in an efficient manner and to hold intermediate results (lists of suspects that have yet to be eliminated through "intersection"). These requirements become more complex when people make use of multiple Internet connection providers to connect to remote services.
23. Furthermore, if an inquiry proceeds in a 'snowball' manner – identify who is using this account, see what else they are using, find all the other users of those services, rinse and repeat – then making lots of individual data requests to providers is clearly inefficient.
24. That appears to be what clause 51 et seq. is addressing – the data will be accessible from a central system which can perform the necessary database operations to slice and dice the data to pull out the relevant list of suspects.
25. It is a mere implementation detail (an engineering trade-off) whether the ICR data record are actually moved to a central location or whether there is merely a standard interface by which the central system can request small subsets of the data. It may look as if an ISP or telco is 'in control of their data' if the vast bulk of it continues to reside solely on their disks in their own data centre, but in practice they will have no idea (and no practical means of monitoring) what queries are being made against it.
26. The discussion of the filtering system in the explanatory notes concentrates entirely on privacy – stressing that the intermediate results of searches are not processed by humans. This is of course correct (and laudable), but the real reason for the existence of the filter is to allow very rapid and very complex searches to be done across multiple

Internet connection providers and for links between people to inferred very rapidly from very large amounts of data.

27. It seems likely that the filter will not hold just ICR data but also large amounts of other data – geotracking, vehicle movements from the ANPR system, phone call records etc. because the analysts who use it will want to cross-correlate data, for example to identify 'fellow travellers' (those in the same car as a suspect), and many other imaginative ways of tracking and surveilling the population.

What's wrong with the Bill (a technical perspective) ?

28. A key technical problem with this Bill is that, like the legislation that preceded it, the wording is entirely prescriptive rather than descriptive. This has two key consequences, the first is that I predict that the provisions will turn out to be just as fragile as previously and technology change will mean that they will require rapid revision. The second consequence is that unless you are an expert, or have consulted with experts, it is entirely opaque as to what type of activity will be made lawful.

29. What I mean by the wording being prescriptive is the Bill continually says that the Secretary of State should be allowed to require some general capability X to come to pass, with the exact details of X left for secondary legislation or just the writing of letters to the Internet access companies.

30. A far better way of proceeding would be to put on the face of the Bill the questions that the providers of Internet access are to be required to be able to answer upon the receipt of appropriate paperwork.

31. For example the Bill might specify (in appropriate statutory language): "given logs from a remote service you should be able to identify which of your customers was responsible for an event".

32. The Home Office's current approach to getting the answer to this question is to require companies to hold ICRs (which may not actually work out this time, see #7 above). However, back in 2005 they wanted IPs logged (which worked OK for cable and ADSL, but didn't work for the mobile carriers) or just last year they wanted logging of source ports (which hasn't been a success).

33. If the requirement on the face of the Bill was for all Internet access providers to be able to answer a specific question then they can decide for themselves how best to do this. As the technology changes the way they provide the answers would then be automatically updated by them without further regulation. Indeed, if this had been the requirement in 2005 (or 2014) then much of the current Bill could have been copied in from earlier legislation instead of being rewritten from scratch.

What's wrong with the Bill (a social perspective) ?

34. If Law Enforcement wish to go well beyond 'reverse directory lookup' into the types of surveillance which were previously only available by using interception then putting this on the face of the Bill would enable proper debate about the appropriateness of the power and the level of authorisation to be required, which ought in my view to be very similar to the authorisation required for interception.

35. The present Bill forbids almost nothing (not just in the topics I have discussed, but throughout) and hides radical new capabilities behind pages of obscuring detail.
36. This is a major problem for proper discussion of the suitability of what is being proposed. For just one example, the appropriateness of snowball searches (and what level of authorisation might be required) is most unlikely to be properly debated by the public or within Parliament when it requires careful analysis of the Bill and guidance from experts before it even becomes apparent that these searches are to be allowed.
37. To take another example – the use of the filter to identify 'fellow travellers' is unsurprising to technical experts: it's just a simple correlation. It's unsurprising to those who have read the documents that Snowden has leaked because some forms of this are described therein. However, if in the future it comes as surprise to the public at large then we are putting the notion of 'policing by consent' at serious risk.
38. If we are going to give Orwellian powers to Law Enforcement then we should fully debate this change to our relationship with the state, not just make all the capabilities (and more) of a classic police state lawful and somehow trust that either Law Enforcement will not realise what they can now do, or that random police Superintendents will always make the right decisions about necessity and proportionality to maintain our free society.

Dr Richard Clayton
University of Cambridge
21 December 2015

Naomi Colvin—written evidence (IPB0063)

I work for the Courage Foundation, an international organisation that supports individuals who risk life or liberty to make significant contributions to the historical record. One of our beneficiaries is Edward Snowden. I am writing this submission in a personal capacity.

I have many concerns about the substance of the Draft Bill but will focus on the new offences that have been proposed, whether they are necessary and whether the penalties are appropriate.

In my opinion these new offences seem likely to limit public understanding of the way investigatory powers are used and curtail the ability of whistleblowers and security researchers to raise valid concerns. This would be a particularly unfortunate outcome given the vital role Edward Snowden has played in bringing us to this point.

Separately, while I welcome the introduction of special protections for journalists' communications data, these do not go far enough to protect the identities of sources, who would clearly be at risk of being exposed incidentally even if they are not the focus of a particular investigation. As I anticipate you will be receiving comments from others on this issue, I do not discuss it further in this submission.

In summary:

- As a general principle, prohibitions on the disclosure of investigatory powers orders should be limited to what is strictly necessary for operational purposes.
- The Draft Bill significantly expands the scope of existing prohibitions on disclosure and I do not see that the case has been made for this.
- Even before Edward Snowden's revelations, international organisations recognised that a public interest defence needs to be available for whistleblowers. This is missing from the Bill as it stands.
- In their present form, the new offences in the Draft Bill risk criminalising, not just whistleblowers, but security researchers who expose breaches of network security in the public interest.
- Specific protections for journalists and others dealing with confidential information are a welcome step forward but will not provide sufficient protection.

Recommendations:

- Clause 66 should be reframed so that permanent secrecy is the exception, rather than the general rule.
- Aggregate data on the use of all investigatory powers should be published at regular intervals, as IOCCA does currently for communications data requests.
- CSPs should not be prevented from publishing their own transparency reports.
- The scope of data retention orders (clause 77) should remain public.
- An explicit public interest defence should be included in the Bill, which would protect both whistleblowers and security researchers working in the public interest.

- No request should be made for the content or metadata of journalists or others dealing with confidential information without a full judicial assessment of necessity and proportionality

The proposed offences

1. Of the three major reports into the UK's investigatory powers and oversight arrangements that followed Edward Snowden's surveillance revelations, the only recommendation for a new criminal offence is in the Intelligence and Security Committee's report, which called for a new offence of misusing surveillance powers. This recommendation has been reflected in a new criminal offence of "wilful or reckless use of communications data" at Clause 8 in the Draft Bill.

2. However, the majority of the new, or broadened, offences in the Draft Bill concern the unauthorised disclosure of a variety of government orders and, on this subject, the ISC actually called for greater openness. Concerning targeted warrants the ISC recommended that, contrary to the blanket prohibition under RIPA, "disclosure [of a specific interception warrant] should be permissible where the Secretary of State considers this could be done without damage to national security."

3. Given the lack of any call for new offences on disclosure, it is surprising that the extensive documentation published alongside the Draft Bill gives only limited guidance about the intention behind these new, and expanded, offences. Several have been put forward without any explanation at all. Where motivation has been given, the wording in the Draft Bill appears to be framed more broadly than required for that purpose.

4. Clause 44(2)(a) in the Draft Bill creates an offence of making an unauthorised disclosure about a targeted interception warrant. The maximum punishment for this offence is five years' imprisonment and a fine. This is substantially similar to the current situation under Section 19 of RIPA.

5. Clause 66 makes it an offence for "a telecommunications officer, or any person employed for the purposes of the business of a telecommunications officer" to disclose information about a targeted notice for communications data. This carries a potential penalty of two years in prison and a fine. This is a new criminal offence. Under RIPA Section 22, there is a duty for a postal or telecommunications provider to comply with a communications data notice, but this is enforced with civil proceedings, not criminal ones.

6. Clause 102 makes similar provision in relation to equipment interference warrants and the steps required in order to implement them. As equipment interference has only been recently avowed, this offence is new and - as with communications data notices - carries a potential penalty of two years in prison and a fine.

7. The Draft Bill introduces three new offences regarding to operations conducted in bulk. Clause 120 introduces an offence of unauthorised disclosure about the existence or facilitation of a bulk interception warrant and related communications data. Clause 148 makes similar provision regarding the disclosure of a bulk equipment interference warrant. These new offences each carry a potential penalty of five years in prison and a fine. Clause

133 makes similar provision regarding the bulk communications data, with a maximum penalty of two years' imprisonment and a fine. Finally, Clause 190 prohibits the disclosure of a Technical Capability Notice or a National Security Notice.

Has the case been made?

8. Clause 66 is one of the few new offences to be discussed in the various documents released alongside the Bill. The Explanatory Notes state that new criminal offence of disclosing a communications data order is designed to prevent criminal suspects or people of interest being "tipped off" that they are under investigation. The Impact Assessment for Communications Data notes that there are cases where the disclosure of a data request would not be detrimental to an investigation, but it is only possible for CSPs to alert their customers "in such circumstances where a public authority is content for them to do so."

9. The Privacy Impact assessment, also published alongside the Draft Bill, is framed more permissively:

10. "Under new legislation, there will not be an absolute prohibition on communication service providers from disclosing to their users that they are subject to a communications data request unless it will affect the operation."

11. I agree with the principle that the prohibition on the disclosure of targeted warrants should not be absolute, but instead linked to operational necessity. The language of the Bill, however, does not achieve this aim very effectively. Creating a new criminal offence here sends out exactly the opposite message.

12. The experience of other countries shows that a proper system of user notification is perfectly practical. Instead of creating a general prohibition backed up with criminal sanction with a limited allowance for "expressly permitted" exceptions, it would be better if Clause 66 created a general rule about when orders can be disclosed, subject to continued confidentiality on a case-by-case basis where it is required.

13. In this way, those whose data has been acquired illegitimately would be in a better position to seek redress than they are at present. Currently the only remedy available to individuals in the UK is to make an application to the Investigatory Powers Tribunal, which will only confirm whether an unlawful operation has taken place. There is no mechanism whereby those who do not suspect themselves to have been unlawfully surveilled would ever discover what has happened. As a result, the proposed offence under Clause 8 of the Draft Bill is not likely to command public confidence.

14. **The Committee should consider whether Clause 66 in particular would be better framed as a general expectation that orders for communications data will become public at some point in the future, subject to an official veto where it is operationally necessary.**

15. A second concern is that the language of the Draft Bill is broader than necessary - in each of the three provisions relating to targeted warrants, the criminalised behaviour is not notifying the subject of a notice, it is notifying "anyone."

16. The breadth of this language may inadvertently prevent communications service providers from releasing aggregated, anonymised information about the official requests they receive. In recent years, an increasing number of communications service providers have started releasing transparency reports, which have done a great deal to improve public understanding.255

17. In the aftermath of Edward Snowden's revelations a number of CSPs in the United States reached an agreement with the US Department of Justice, allowing data on official orders to be disclosed in a set format.256 Enabling CSPs to release this kind of comparative data would provide an important complement to the very valuable information currently issued by IOCCA and the US agreement provides a possible model to follow.

18. **Nothing in these provisions should prevent CSPs producing their own Transparency Reports. Where such international, anonymised and aggregated data is available, this provides an important complement to the information issued by public authorities.**

19. For bulk orders, "tipping off" is obviously not a concern. Given that, by their nature, such orders will affect a very large number of people who are not suspected of any wrongdoing, a permanent prohibition on revealing anything about these orders, which are matter of active public concern, seems disproportionate and likely to inhibit future policy discussion.

20. Based on the oral evidence heard by the Joint Committee on 16 December, there is a significant gap in public knowledge about how equipment interference powers are being used and their frequency. This is a key example of where we need much greater information in the public domain and to curtail public debate at this point is clearly not justified.

21. **There should be consideration of how the use of bulk orders and equipment interference powers can be reported so as not to inhibit public understanding of how they are being used. At the very least, statistics on their use should be published periodically.**

Retention notices

22. Section 77 introduces a duty for "a telecommunications operator, or any person employed for the purposes of the business of a telecommunications operator" not to disclose the existence or content of a data retention notice. While the duty to comply with a data retention notice is not new, the duty to keep secret the "contents" of such a notice certainly is - under the Data Retention and Investigatory Powers Act (2014), augmented with a provision in the Counter Terrorism and Security Act (2015), the categories of data that ISPs are obliged to retain are explicitly set down in law. The Draft Bill is considerably more

[255]See, for instance, Vodafone's Law Enforcement Disclosure Report, released in February 2015 https://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html#eocp

[256]https://www.washingtonpost.com/business/technology/us-to-allow-companies-to-disclose-more-details-on-government-requests-for-data/2014/01/27/3cc96226-8796-11e3-a5bd-844629433ba3_story.html

opaque in this respect, not least due to the ambiguity as to what constitutes an "internet connection record."

23. A strong case needs to be made for imposing secrecy where information has formerly been available to the public, particularly in a matter which potentially impacts everyone who uses a British ISP. The desire to "future proof" legislation should not leave the public in the dark about the ways powers are used now and how that may change in the future.

24. **The case has simply not been made for an expansion of secrecy in this area. The scope of data retention orders should remain public.**

A public interest defence

25. The Council of Europe and other standards-setting bodies have been moving in the direction of a public interest defence for all whistleblowers, including those whose disclosures impact on matters of national security. While none of these statements are legally binding, there is real momentum in this area, which has increased since Edward Snowden's revelations started in summer 2013.

26. The Global Principles on National Security and the Right to Information (the Tshwane Principles) were first published on 12 June 2013, six days after the first report based on Edward Snowden's revelations was published, but after two years of work. The Tshwane Principles are based on a survey of national and international legal standards and informed by discussions with 500 experts from 70 countries.

27. The Tshwane Principles provide guidance on categories of information of "high public interest", which includes statistics on the extent of surveillance practices. The Principles also state that whistleblower protections should be extended to national security disclosures under certain conditions (such as, for example, a previous attempt to report concerns within an organisation, where adequate provision exists to do so), but that in any case disclosures in the public interest should be protected from retaliation. Where individuals are prosecuted for the disclosure of information over and above that required in the public interest any punishment should be proportional to harm caused by the disclosure.

28. The Parliamentary Assembly of the Council of Europe (PACE) endorsed the Tshwane Principles in October 2013. The Committee of Ministers has also adopted a recommendation257 on the Protection of Whistleblowers that recognises that, while member states may institute "a scheme of more restrictive rights" for information related to national security, defence or international relations, "they may not leave the whistleblower completely without protection or a potential defence." In a resolution of May this year, the Parliamentary Assembly went further and recommended asylum should be available for national security whistleblowers whose disclosures have not been treated in accordance with the Tshwane Principles.258

[257] (CM/REC(2014)7

[258] Committee of Legal Affairs and Human Rights Doc 13791, 19 May 2015

29. David Kaye, the UN Special Rapporteur for the Promotion and Protection of the Right to Free Expression, in his report of 8 September 2015 concurred that states should avoid prosecuting whistleblowers but, where this happens, defendants "should be granted ... the ability to present a defence of an overriding public interest in the information and ... access to all information necessary to mount a full defence, including otherwise classified information."259

30. In March 2014, the European Parliament adopted the conclusions of an inquiry into surveillance practices conducted by the LIBE committee. Among its many recommendations, this report recommended that the European Commission consider the possibility of establishing guidelines for national security whistleblowers across the EU and called on member states to ensure their national frameworks were in accordance with international standards, including the Tshwane Principles.

31. Recent comparative studies of G20 countries describe the status of national intelligence and defence in the UK as a "glaring gap" in the legal framework protecting whistleblowers.260 Without amendment, the new offences in the Draft Bill will have the effect of widening the scope of that gap to make CSP employees and contractors subject to Official Secrets Act-type restrictions and penalties.

32. An explicit public interest defence is also necessary to make the equipment interference offences workable. There is a clear tension between the ability to issue an order to anyone with “access” to a desired resource and imposing a duty on all employees of a communications service to keep an order, or the steps needed to fulfil an order, secret – it is far from clear that those two groups would have a working relationship with each other, still less work for the same company.

33. This also creates legal ambiguity around the basic practices of computer security research, whereby freelance computer security experts search for, analyse and report on vulnerabilities in the systems of technology firms, sometimes in response to "bug bounties". This practice has been recognised by the world's most prominent technology companies, such as Google and Facebook, as an integral part of the day to day assurance of network security, and as necessary to protect technology consumers and the smooth functioning of the industry.

34. A growing area of research has revealed how human rights defenders have been targeted with equipment interference attacks using commercial surveillance tools acquired by nation states. This work is very clearly in the public interest.261

35. Researchers working in this field already face legal uncertainty. The wording in the present bill expands this ambiguity, potentially criminalising important work, or creating strong disincentives against it taking place.

---

259 A/70/361, paragraph 65

260 See https://blueprintforfreespeech.net/G20

261 See, for example, https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists/

36. An explicit public interest defence should be included in the Bill, which would protect both whistleblowers and security researchers working in the public interest.

20 December 2015

Committee on the Administration of Justice ('CAJ')—written evidence (IPB0025)

The Bill and the Northern Ireland peace settlement: should the legislation deal with CHIS and undercover officer conduct too?

Committee on the Administration of Justice ('CAJ')

1. CAJ is an independent human rights organisation with cross community membership in Northern Ireland and beyond. It was established in 1981 and lobbies and campaigns on a broad range of human rights issues. CAJ seeks to secure the highest standards in the administration of justice in Northern Ireland by ensuring that the Government complies with its obligations in international human rights law.

2. CAJ welcomes the opportunity to provide Written Evidence to the Joint Committee on the Draft Investigatory Powers Bill. The bill provides a new framework for the use of investigatory powers, with a focus on surveillance. Outside of the issues with the current bill **CAJ wishes to draw attention to other areas of covert policing where there is currently inadequate regulation** under the Regulation of Investigatory Powers Act 2000 (RIPA), **namely regulation of the permitted behaviour of informants (Covert Human Intelligence Sources- CHIS) and undercover officers.**

3. The purpose of our submission is to seek to promote debate around the potential to legislate in this area to remedy deficiencies in RIPA and implement unmet commitments in the Northern Ireland peace settlement. These issues are found in outstanding recommendations from the Independent Commission on Policing in Northern Ireland (the Patten Report),[262] the Police Ombudsman's Operation Ballast Report[263] and the Desmond de Silva Review into the death of Pat Finucane.[264]

4. Whilst RIPA does introduce an authorisation system for CHIS it does not adequately provide for regulating the conduct of CHIS and in particular the extent to which CHIS are permitted to be involved in crime. Our view is that the law should codify and prohibit CHIS and undercover officer involvement in human rights violations. The de Silva review concludes that such a system is not in place under RIPA stating:

> ...it is doubtful whether RIPA and its associated Code of Practice provides a real resolution to these difficult issues given that it provides little guidance as to the limits of the activities of covert human intelligence sources (para.4.88).

5. The Cabinet Office response to the de Silva Review sets out:

> De Silva acknowledges the improvements made as a result of RIPA and its Code of Practice. However, he argues that these do not provide adequate

[262] 'A New Beginning: Policing in Northern Ireland'. The Report of the Independent Commission on Policing in Northern Ireland' (Patten Report) September 1999,

[263] 'Statement by the Police Ombudsman for Northern Ireland into her investigation into the circumstances surrounding the death of Raymond McCord Jr and related matters' (Operation Ballast Report), Nuala O'Loan, Police Ombudsman for Northern Ireland, 22nd January 2007

[264] The Report of the Patrick Finucane Review, The Rt Hon Sir Desmond de Silva QC, December 2012, HC 802-I.

guidance as to the limits of the activities of CHIS in criminality. Since he wrote his report, additional CHIS oversight has been put in place, including reinforcement of the RIPA framework. Where, in exceptional circumstances, it proves necessary for CHIS to participate in criminal acts in order to fulfil their authorised conduct, agencies giving such tasking will only carry out such operations subject to the most stringent processes and safeguards.[265]

6. The Police Ombudsman's 2007 Operation Ballast Report, which uncovered practices of collusion with loyalist paramilitaries, enumerates a number of safeguards introduced in the Police Service of Northern Ireland (PSNI) since the initiation of the Ballast investigation itself. The PSNI instigated a 'major review' (the CRAG Review) of informants in 2003 which resulted in around a quarter of all informants being let go; half of them as they were deemed "too deeply involved in criminal activity".[266] The Report states the review directed that "all criminal activity by paramilitary informants has to be strictly documented and controlled" and that "The CRAG review established that involvement in any criminal offence, other than membership or support of a proscribed organisation, had to be the subject of an application to the ACC of Crime Operations, who would approve or refuse the request. ..." There is now therefore a system of covert deployment authorisations, whereby the ACC must authorise the involvement of an informant in any criminal offence over and above membership or support of a paramilitary organisation.[267] There was also the adoption of a Manual for the Management of CHIS and other safeguards. **However, at present all these developments and the framework they provide are not reflected in RIPA or its associated codes of practice.**

7. It is has never been made public if equivalent measures to those adopted by the PSNI were also introduced for the Security Service MI5 when it took over primacy for 'national security' covert policing in Northern Ireland in 2007.[268] CAJ was recently told by Lord Carlile, non-statutory Reviewer of the National Security Arrangements in Northern Ireland, that the Security Service has introduced a policy framework for CHIS handling over and above the provisions of RIPA. Lord Carlile also stated that the system would not authorise CHIS involvement in actions which would violate ECHR Article 3, such as 'punishment beatings'. Given the stated existence of such policy we cannot see any reason why such a policy framework precluding CHIS and undercover officers from engaging in acts which would constitute human rights violations not be explicitly placed on a statutory footing and hence put in the public domain.
8. There are other areas whereby accountability for this area of covert policing falls short of what was committed to under the peace settlement. The **Patten Report** stated that Police Codes of Practice should be publicly available[269] and that Codes of Practice on all aspects of policing, **including covert law enforcement techniques**,

[265] Lessons learnt by government departments from Sir Desmond de Silva's Report of the Patrick Finucane Review A report by the Cabinet Secretary, the Secretary of State for Defence and the Secretary of State for Northern Ireland (Cabinet Office, 2015), paragraph 10.
[266] Operation Ballast Report, Appendix A, paras 8-10.
[267] Operation Ballast Report, Appendix A, paras 14-15.
[268] For detailed account of the transfer see *CAJ 'The Policing You Don't See' December 2012*.
[269] Patten Report, paragraph 6.38.

should be in strict accordance with the ECHR.[270] In relation to police Codes of Practice being publicly available Patten stated:

> ...this does not mean, for example, that all details of police operational techniques should be released – they clearly should not – but the principles, and legal and ethical guidelines governing all aspects of police work should be, including such covert aspects as surveillance and the handling of informants...**The presumption should be that everything should be available for public scrutiny unless it is in the public interest – not the police interest – to hold it back...**Transparency is not a discrete issue but part and parcel of a more accountable, more community-based and more rights-based approach to policing (emphasis in original).[271]

9. To date no document setting out the ethical boundaries of informant conduct has been provided for in legislation or otherwise published. Patten also recommended *A Commissioner for Covert Law Enforcement in Northern Ireland.*[272] This Commissioner was also never introduced.[273] Potentially such an office could consolidate and replace the array of existing Commissioners overseeing such work with more limited powers.

10. In summary CAJ wishes to draw attention to other areas of covert policing that are in urgent need of legislative reform to ensure they are being undertaken in a human rights compliant manner. We would like to see provisions in legislation which explicitly prevent the authorisation of CHIS or undercover officer participation in activities which would constitute, as agents of the state, human rights violations.

17 December 2015

[270] Patten Report, paragraph 4.8.
[271] Patten Report, paragraph 6.38.
[272] Namely: "...a senior judicial figure, based in Northern Ireland, whose remit should include surveillance, use of informants and undercover operations... [with] powers to inspect the police (and other agencies acting in support of the police) and to require documents or information to be produced, either in response to representations received, directly or through the Police Ombudsman, the Policing Board or others, or on his or her own initiative. The commissioner should ... conduct sufficient inquiries to ascertain whether covert policing techniques are being used: with due regard for the law; only when there is a justification for them; and when conventional policing techniques could not reasonably be expected to achieve the objective. The commissioner should check that justifications for continuing specific covert operations are regularly reviewed, and that records of operations are maintained accurately and securely, with adequate safeguards against unauthorised disclosure." (Patten Report, paragraph 6.44).
[273] S61 of RIPA 2000 introduced an Investigatory Powers Commissioner for Northern Ireland, but this is not the role envisaged by Patten and instead relates to non-police powers. Furthermore, we were previously informed nobody has actually been appointed to this office.

Ray Corrigan—written evidence (IPB0053)

My name is Ray Corrigan. I'm a Senior Lecturer in the Maths, Computing & Technology Faculty of The Open University, though I write to you in a personal capacity.

Summary

The Joint Committee is being required to analyse the long and complex Draft Investigatory Powers Bill in an unreasonably short timescale.

This submission to your inquiry is divided into 6 sections covering:

- Bulk collection & retention of personal data by computers
- Privacy
- Legality of bulk collection and retention
- ICRs and relevant communications data
- The base rate fallacy and the lack of efficacy of bulk data collection
- Complex system security and equipment interference

The first section challenges a fundamental misunderstanding – the idea that collecting and retaining bulk personal data is acceptable as long as most of the data is only "seen" by computers and not human beings. This is a line that has been promoted by successive governments for some years and seems to be widely accepted. Yet it is seriously flawed.

Next I suggest a simplified version of US scholar Daniel Solove's model of privacy, to help provide a framework for thinking about information and data processing, in the context of communications surveillance.

Then the April 2014 European Court of Justice Digital Rights Ireland decision, invalidating the Data Retention Directive, is reviewed. Viewed carefully, the decision could be considered an aid to framing surveillance legislation. The draft Investigatory Powers Bill in its current form would be unlikely to meet the tests, laid down in the case, regarding compatibility with privacy and data protection rights, guaranteed by articles 7 and 8 of the EU Charter of Fundamental Rights.

The fourth section examines the tangled web of "internet connection records" and "relevant communications data". Technology law expert, Graham Smith, has identified and mapped 14 different interlinked definitions in the Bill that are connected to "relevant communications data". It is difficult to see how the bulk retention of data under the broad and dynamic scope of "relevant communications data" or "internet connection records" could meet the tests of necessity or proportionality laid down in the Digital Rights Ireland case.

The penultimate section looks at the base rate fallacy, a statistical concept that policy makers must familiarise themselves with if intending to approve the indiscriminate bulk collection, retention and processing of personal data. Finding a terrorist is a needle in a haystack problem. You don't make it easier to find him/her by throwing industrial scale

levels of the personal data, of mostly innocent people, on your data haystack. Section 150 of the Bill, Bulk personal datasets: interpretation, states "the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service in the exercise of its functions". Explicit recognition innocent people would be subject to indiscriminate surveillance under proposed powers.

The final section discusses security in general and the inadvisability of giving government agencies the powers to engage in bulk hacking of the internet. It is advocated that targeted surveillance practices are more effective than mass surveillance approaches and recommended that Part 6, Chapter 3 of the draft Bill be removed in its entirety.

I conclude with an appeal to frame surveillance laws within the rule of law, rather than attempting to shape the law to accommodate expansive, costly, ineffective and damaging population-wide surveillance practices.

Bulk collection & retention of personal data by computers

1. To begin I would just like to note that it is a mammoth task to expect parliamentarians to analyse this long and complex Bill in the short timescale you have been given.

2. I would also like to tackle a fundamental misunderstanding at large in Westminster – the idea that collecting and retaining bulk personal data is acceptable as long as most of the data is only "seen" by computers and not human beings; and it will only be looked at by persons with the requisite authority if it is considered necessary. This is a line that has been promoted by successive governments for some years and seems to be widely accepted. Yet it is seriously flawed.

3. The logical extension of such an argument is that we should place multiple sophisticated electronic audio, video and data acquisition recording devices in every corner of every inhabited or potentially inhabited space; thereby assembling data mountains capable of being mined to extract detailed digital dossiers on the intimate personal lives of the entire population. They won't be viewed by real people unless it becomes considered necessary.

4. Indeed with computers and tablets in many rooms in many homes, consumer health and fitness monitoring devices, interactive Barbie dolls, fridges, cars and the internet of things lining up every conceivable physical object or service to be tagged with internet connectivity, we may not be too far away from such a world already.[274]

5. The Home Office, on 16 December 2015, rejected a freedom of information request[275] asking for the "metadata of all emails sent to and from the Home

[274] Executive Office of the President President's Council of Advisors on Science and Technology Report to the President, [May, 2014], Big Data and Privacy: A Technological Perspective

[275] https://www.whatdotheyknow.com/request/300685/response/745953/attach/html/3/FOI%2037410%20Response.pdf.html

Secretary for the period 1st January 2015 - 31st January 2015 inclusive." They rejected the request on the grounds that the request "is vexatious because it places an unreasonable burden on the department, because it has adopted a scattergun approach and seems solely designed for the purpose of 'fishing' for information without any idea of what might be revealed."

6. Yet the same Home Office considers it acceptable to have powers, in the Investigatory Powers Bill, to engage in bulk data collection, retention and equipment interference, to assemble information about every member of the population, in the hope of conducting contemporaneous and/or post hoc 'fishing' activities to look for evidence of misbehaviour.

7. I would contend that this approach is unnecessary, disproportionate and incompatible with the rule of law. It is additionally very costly and technically, mathematically and operationally ineffective. If all that was not bad enough, it risks undermining the security of our already frail and insecure communications infrastructure.

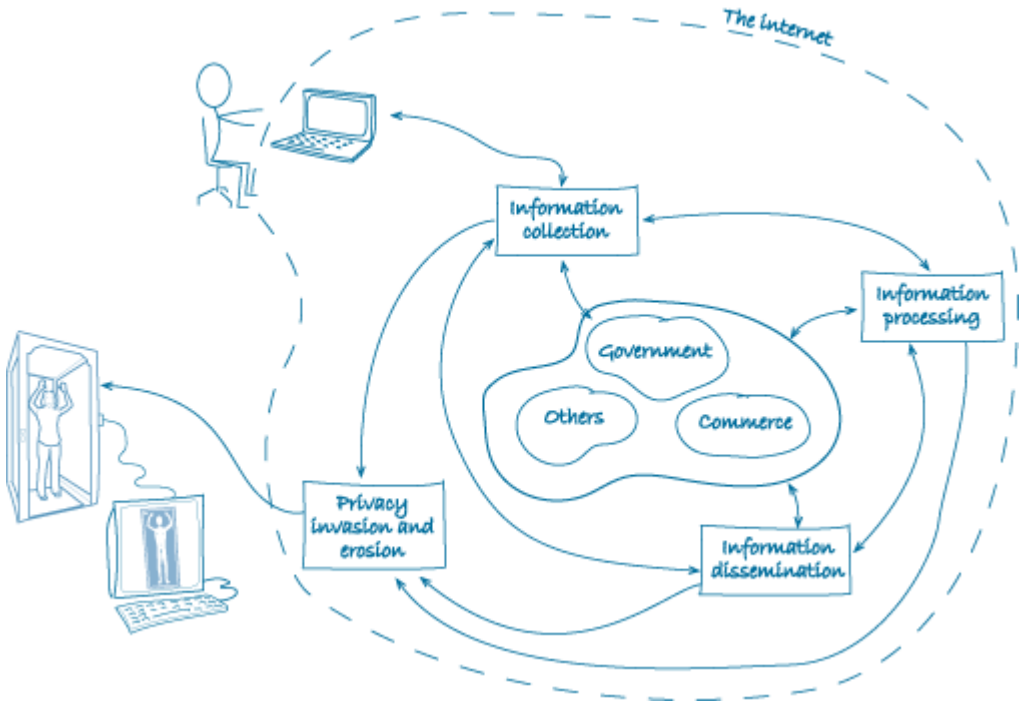
Privacy

8. Individual and collective privacy underpins a healthy society but privacy is hard to define. We understand the conceptual protection of a person's home being their castle and what is behind closed doors being private. But privacy was the default state in the pre-internet world and we didn't think too hard about its subtleties. With mass personal data processing, however, we need a better understanding of privacy. US scholar Daniel Solove has helpfully characterised privacy as a collection of problems.[276] Privacy harm, Solove argues, is triggered by –

    - Information collection
    - Information processing
    - Information dissemination/sharing
    - Privacy invasion and erosion

9. We now teach a simplified model of Solove's taxonomy to our 3rd level information systems students at The Open University a visual depiction of which I include below.

[276] Solove, DJ, [2006], A Taxonomy of Privacy, University of Pennsylvania Law Review, Vol.154 No.3



10. One of the key issues clarified by Solove's model is that the initial privacy harm originates at the point of collection of personal data, whether that collection is done by a computer, other device or a person. In the context of investigatory powers it can be helpful to ask whether the specifics under consideration relate to information collection (& retention), information processing, information dissemination or privacy invasion. Whichever of these processes are at issue their collective effect is the stripping bear of the digital persona of anyone who comes into contact with devices connected to the internet.

11. *Information collection* is the surveillance done by commerce, governments and other agents, such as criminal gangs. Solove suggests it also covers the interrogation of the information collected.

12. Commerce, governments and others are involved in *information processing* – the storage, use (or misuse), analysis and aggregation of lots of data, secondary use of data, the exclusion of the data subject from knowledge of how information about them is being used and exclusion from being able to correct errors. Solove expresses particularly concern about bureaucracy. Surveillance bureaucracy makes life-changing decisions based on secret information, while denying the subject/s of the data the ability to inform, see or challenge the information used. The privacy problem here is all about information. The privacy harms are bureaucratic – powerlessness for the subject, indifference to them, error, lack of transparency and accountability.

13. On that front, when giant data mountains are conveniently sitting around, there is not a safeguard in existence that will prevent (possibly even well-intentioned) future incarnations of a bureaucracy from tapping that data for secondary uses not

originally envisaged by those behind the IP Bill. A related case in point is the expansive interpretation of s7(4) of the Intelligence Services Act 1994 and the Equipment Interference Code of Practice 2015 to justify the equipment interference activities currently undertaken by the security and intelligence services (SIS). Provisions for equipment interference and bulk equipment interference included in part 5 and 6 of the IP Bill present serious economic wellbeing and security risks.

14. *Information dissemination* – Data viewed out of context can paint a distorted picture. The novelist researching criminal behaviour might be flagged for buying too many of the wrong kinds of books from an online bookshop. In the UK collection of information 'of a kind likely to be useful to a person committing or preparing an act of terrorism' is a criminal offence, under Section 58 of the Terrorism Act 2000. We might expect an analyst to recognise a known novelist but processing purely by algorithm may lead to distortion and faulty inference. We also get dissemination through leaking and misappropriation through stealing of personal information, which can lead to exposure to identity theft, fraud, blackmail, and further distortion.

15. *Privacy invasion* is about the information activities and their aggregation mentioned above but also amounts to intrusion into the personal sphere. Overt surveillance, direct interrogation, junk mail, unsolicited phone calls are all disruptive intrusions and cause harm. But there can be a decision making element to this intrusion too. For example someone may be reluctant to consult a doctor if current plans on the sharing of health data through the ill-considered care.data scheme progress further. Innocents may be inhibited from using the internet if they feel under constant surveillance.

16. Whether or not mass indiscriminate personal data collection and retention is only "seen" by computers it remains mass indiscriminate personal data collection and retention, repeatedly found unlawful by the Court of Justice of the European Union [Digital Rights Ireland, 2014; Schrems 2015], the European Court of Human Rights [Zakharov, 2015] and multiple high courts including Romania (2009), Germany (2010), Bulgaria (2010), the Czech Republic (2011) and Cyprus (2011). Mass indiscriminate personal data collection and retention has been variously described by these courts as unconstitutional and/or a disproportionate unjustified interference with the fundamental right to privacy, free speech and confidentiality of communications.

Legality of bulk collection and retention

17. On 8 April2014 the Grand Chamber of the European Court of Justice, (ECJ) in joined cases C-293/12 and C-594/12, issued a landmark decision declaring the 2006 data retention directive invalid. The Grand Chamber of the Court effectively condemned pre-emptive, suspicionless, bulk collection and retention of personal data and consequent "interference with the fundamental rights of practically the entire

European population". The Paragraph 37 of the judgment noted the interference with articles 7 (data protection) and 8 (privacy) of the EU Charter of Fundamental Rights caused by mass data retention “must be considered to be particularly serious.”

18. Paragraph 58 of the decision criticises the mass surveillance of innocent people not remotely connected to serious crime. Then in recognition of the need for targeted rather than mass surveillance the Court states:

> "59. Moreover, whilst seeking to contribute to the fight against serious crime, Directive 2006/24 does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences."

So the Court considers it unnecessary and disproportionate to engage in bulk collection of innocent communications in order to find serious criminals.

19. Finding a terrorist or serious criminal is a needle in a haystack problem – you can’t find the needle by throwing infinitely more needle-less electronic hay on the stack. Law enforcement, intelligence and security services need to use modern digital technologies intelligently in their work and through targeted data preservation regimes – not the mass indiscriminate data collection, retention and equipment interference proposed in the Investigatory Powers Bill – engage in technological surveillance of individuals about whom they have reasonable cause to harbour suspicion. That is not, however, the same as building an infrastructure of mass surveillance or facilitating the same through the legal architecture proposed in the Bill.

20. The ECJ follows up this mass surveillance critique with a clear declaration in paragraph 60 that the data retention directive had no limits on access to and use of retained data to the purpose of fighting serious crime and no criteria for determining such limits. Paragraphs 60 to 68 could be read as a lesson on how to write a data retention law in a way that might be acceptable to the Court. The data retention directive declared invalid by the Court did not –

- include procedures on determining access to data or its use or even limiting these to crime fighting
- limit the number of people with access to the retained data to those strictly necessary
- subject access to the data to the prior review or oversight of a court, in order to limit access to that which is strictly necessary
- oblige member states to set down such procedures.

- make any distinction between categories of data
- attempt to justify the arbitrary period of retention chosen of between 6 months and 2 years
- lay down clear and precise rules governing the extent of the interference with the fundamental rights to privacy and data protection
- provide for sufficient safeguards to ensure effective protection of the data retained against the risk of abuse
- provide for sufficient safeguards to ensure against any unlawful access and use of that data
- specify a high enough data security threshold
- require the irreversible destruction of data at the end of the retention period
- require data to be retained within the borders of the EU
- ensure control of data protection and access to the retained data by independent authority

21. Big and complex as the Investigatory Powers Bill is, it too falls at many of these hurdles in relation to the bulk data collection and retention powers proposed. IT fundamentally fails to take into account data protection principles, in particular data minimisation.[277] Not only does the IP Bill eschew data protection principles, it promises to offer its own version of data processing rules to deal with bulk data which will appear as a code of practice. A guide to what this code of practice will look like is included in Schedule 6, section 3 of the Bill.

22. The Court concluded:

> "69. Having regard to all the foregoing considerations, it must be held that, by adopting Directive 2006/24, the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter.
> 70. In those circumstances, there is no need to examine the validity of Directive 2006/24 in the light of Article 11 of the Charter.
> 71. Consequently... Directive 2006/24 is invalid."

23. In short, the data retention directive presented a disproportionate interference with the fundamental rights to respect for private and family life and the protection of personal data. Consequently the directive was invalid, null and void. And because it was invalid on privacy grounds the Court didn't see the need to pursue the question of whether it also might be invalid on the grounds of Article 11 of the Charter of Fundamental Rights relating to freedom of expression.

Internet connection records and relevant communications data

24. The Home Office appear to have briefed the Joint Committee that the retention of "internet connection records" is the only new power in the Bill. As far as I can tell the phrase "internet connection records" is mentioned only in section 47 of the Bill ("Addition restriction on grant of authorisations") which does not deal with data

[277] https://ico.org.uk/for-organisations/guide-to-data-protection/principle-3-adequacy/

retention. Section 71 (Powers to require retention of certain data) deals with data retention and uses the term "relevant communications data" rather than internet connection records.

25. "Relevant communications data" has a six part definition in s71(9)(a)-(e) relating to the purposes of section 71. "Internet connection record" has a two part definition in s49(6)(a)-(b) relating to that section. The components of the "relevant communications data" definition them acquire different meanings or definitions depending on what part of the Bill they appear in.

26. Graham Smith has done a remarkable job of tracking these down. In a blogpost on Sunday, 29 November 2015, *Never mind Internet Connection Records, what about Relevant Communications Data*[278], he identified and mapped 14 different interlinked definitions in the Bill that are connected to "relevant communications data".

27. It is hardly surprising therefore that industry representatives, such as BT's Mark Hughes, have testified to the joint committee that the definitions in the Bill are unclear.

28. Relating "relevant communications data" back to the Solove model (at the beginning of my submission) implicates it variously in data collection, retention, processing and dissemination. Unfortunately even that doesn't help identify exactly what "relevant communications data" is going to mean in practice.

29. Government representatives have told the joint committee that definitions of ICRs and relevant communications data are "clear" and industry have insisted they are unclear in the Bill. It appears that what they really mean in practice will be worked out in private discussions through the "very good relationship" the government maintains with industry.

30. Does the joint committee get to oversee these discussions? So who gets the final say on who gets to program the computers for surveillances and what are the specific 'selectors'/filters? Who decides what the selectors should be? Who decides who decides what the selectors should be? With the best will in the world most parliamentarians are not technical experts, so how can the committee effectively or Home Secretary or judicial commissioners scrutinise the technical aspects of this work? How do you measure the efficacy of these filters given it is widely known in the tech community how ineffective electronic filters can be? How, when someone is tagged as suspicious via these secret algorithms applied to bulk datasets, does the information on that individual then get further processed? What happens when someone is wrongly tagged and how do they retrieve their innocence and clean bill of electronic health?

[278] http://cyberleagle.blogspot.co.uk/2015/11/never-mind-internet-connection-records.html

31. It is difficult to see how the bulk retention of data under the broad and dynamic scope of "relevant communications data", or "internet connection records" if that is to be the common phrase to be alluded to regardless of its definition in the Bill, could meet the tests of necessity or proportionality laid down by the Court of Justice of the European Union in the Digital Rights Ireland case in 2014. Given that the final text of the EU's new General Data Protection Regulations (GDPR) just been agreed, it will further complicate the committee's efforts in trying to understand the implications of the proposed IP Bill.

32. One last note on this section on the differences of opinion over the clarity or otherwise of the Bill. The drafters of the Bill have gone to some length to try to distinguish communications data (or meta data) from content. Paul Bernal and others have explained to the joint committee why there is no simple way to distinguish the two, given the complex overlapping nature of both e.g. does an email address mentioned in the main text of a document constitute content or communications data. Could I, on this point, just commend to you the presentation of your special adviser, Peter Sommer, from the 2012 Scrambling for Safety conference, Can we separate "comms data" and "content"– and what will it cost?[279]

Base rate fallacy

33. The whole Investigatory Powers Bill approach to signals intelligence – giant magic computerised terrorist catching machine that watches everyone and identifies the bad guys – is flawed from a mathematical as well as operational perspective.
34. Time and again from the dreadful attacks on the US on the 11th September 2001 through to the recent attacks in Paris the perpetrators were previously known to the security services but they lost track of them in the ocean of data noise they were then[280] and are now[281] drowning in.
35. Even if an IP Bill mandated magic terrorist catching machine, watching the entire population of the world, was 99% reliable, it would flag too many innocents for the security services to investigate and swamp the services in unproductive activity.
36. But it is not even as simple as that mathematically. Is your machine 99% reliable at identifying a terrorist, given they are a terrorist? Or is it 99% reliable at identifying an innocent, supposing they are truly innocent? In general your machine will have two failure rates

    - A false positive where it identifies an innocent as a terrorist
    - A false negative where it identifies a terrorist as an innocent

[279] http://www.pmsommer.com/sf2012_sommer_commsdata_content.pdf
[280] The NSA's Call Record Program, a 9/11 Hijacker, and the Failure of Bulk Collection https://www.eff.org/deeplinks/2015/04/nsas-call-record-program-911-hijacker-and-failure-bulk-collection
[281] Intelligence and Security Committee Report on the intelligence relating to the murder of Fusilier Lee Rigby http://isc.independent.gov.uk/committee-reports/special-reports

37. The reliability of your identification further depends on the actual number of terrorists in the population as a whole – the base rate. The problem is particularly acute when the base rate is low. Let's stick with the 99% reliability for both failure rates (though they will rarely be the same – if you adjust your machine to catch more terrorists, it will falsely accuse more innocents; and if you adjust it to catch less innocents it will let more terrorists go). So assume both a false positive and false negative rate of 1%. Suppose also there are 100 terrorists in every collection of 1 million people.[282] Your terrorist catching machine, watching these 1 million, will flag 99 of the 100 terrorists, giving one a free pass; but it also flags 1% of the remaining 999,900 innocents i.e. 9,999 innocent people get tagged as terrorists. So the 99% reliable machine flags 99 + 9999 = 10,098 people for suspicion. Only 99 of these 10,098 are real terrorists, giving your magic machine a hit rate of 99/10098 = 0.0098 approximately. Your 99% reliable machine is not 99% reliable but less than 1% effective at identifying terrorists.

38. The numbers underlying this base rate fallacy[283] – the tendency to ignore known base rate statistical data (e.g. the low probability someone is a terrorist in a large population) in favour of an interpretation of specific data (my magic machine is 99% accurate) that seems as though it might be right – are slightly counter intuitive but need to be understood if you purport to deploy techniques involving the surveillance of entire populations.

39. Denmark, following 7 years of ineffective bulk collection of data equivalent to the IP Bills internet connection records, in 2014 repealed the law requiring the collection and retention of these records.[284] Because of the base rate fallacy and the fact that terrorists are relatively few in number compared to the population as a whole, mass data collection, retention and mining systems, such as those proposed in the IP Bill, always lead to the swamping of investigators with false positives, when dealing with a large population. Law enforcement authorities end up investigating and alienating large numbers of innocent people. That's no good for the innocents, for the investigators or for society. In Denmark, over half a million records per citizen were retained in 2013 but the system proved an ineffective tool for law enforcement and security and intelligence services.

40. If the government has £175 million over ten years (about equivalent to Wayne Rooney's wages and as industry and others have pointed out to the joint committee, this will not come close to paying for what the IP Bill requires) to invest in terrorism prevention, then it would be better spent on more security services people not

[282] Various spokespersons of successive UK governments have referred to 6000 dangerous people at large in the UK, so I've chosen 100 per million as equivalent to 6000 in 60 million.
[283] For a fuller description of the base rate fallacy see Richards J. Heuer, Jr., Psychology of Intelligence Analysis, Chapter 12 Biases in Estimating Probabilities, available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/art15.html
[284] Details available from http://itpol.dk/consultations/written-evicence-ipbill-scitech-committee IP-Pol submission to the Science and Technology Committee inquiry into the Investigatory Powers Bill.

magic terrorist catching computer systems. You need more human intelligence and better targeted and managed signals intelligence.

Complex system security and equipment interference

41. Our communications infrastructure is complex, fragile and insecure. Large and complex systems like the internet are extremely difficult if not impossible to secure. Security is hard and complexity kills it. When you make any changes to complex systems, they produce unintended emergent effects. But it is a really bad idea to undermine the security of an already fragile and insecure communications infrastructure deliberately, by giving government the power to undermine that security directly, through the equipment interference measures in the IP Bill.

42. There *may* be a case [though it has not been made] for carefully targeted and judicially supervised and controlled, necessary and proportionate equipment interference, to pursue known suspects, about whom the intelligence or law enforcement services have reasonable cause to harbour suspicion. That applies generally to the bulk data collection and retention and equipment interference regime of the IP Bill. The requisite authorities need to use modern digital technologies intelligently in their work and through targeted data preservation regimes – not the mass surveillance regime they are currently operating and the government is proposing to expand under the draft IP Bill – engage in technological surveillance of individuals about whom they have reasonable cause to harbour suspicion.

43. Targeted equipment interference does however, compromise digital forensic evidence that may be used in law enforcement cases.

44. Although equipment interference better known as hacking was avowed by the government with the publication of the draft Equipment Interference Code of Practice early in 2015, government legal representatives at the recent Privacy International Investigatory Powers Tribunal hearing denied that the government had yet admitted engaging in bulk equipment interference.

45. The justification for bulk equipment interference appears to be based on stretching interpretations of the Anderson and Intelligence & Security Committee reports, and the Intelligence Services Act 1994 and the Police Act 1997, beyond breaking point. Anderson, in what I consider one of the few weak/evidence-light parts of his otherwise thorough and impressive report,[285] approved of bulk collection and retention of communications data. In no part of the Anderson report is there expressed or implicit approval for bulk equipment interference.

[285] A Question of Trust: Report of the Investigatory Powers Review by David Anderson Q.C., June 2015

46. Government are claiming bulk equipment interference (mass hacking of the internet) is their attempt to "build on recommendations made by David Anderson QC and the ISC". Generally speaking giving the government the power to hack the internet is really bad security hygiene, undermining communications infrastructure for everyone. Professor Mark Ryan of Birmingham University informed the Joint Committee that equipment interference is “a huge power” which would result in innocent people being targeted. Professor Ryan also described it is an "extremely dangerous game".

47. Numerous other computer scientists and security experts, including Jon Crowcroft at Cambridge University, have described the Bill as a hacker charter, a description recognisable in part 5 and part 6, chapter 3 of the Bill. The 2015 Equipment Interference Code of Practice appears to have stretched the meaning of s7(4)(a) of the 1994 Intelligence Services Act's "acts of a description specified in the authorisation" to mean it covers bulk hacking. Section 7.11 of the Code of Practice claims s7(4)(a) "may relate to a broad class of operations" i.e. anything? Part 6 Chapter 3 would appear to be aimed at codifying this in the new law.

48. There is no case for the open ended bulk equipment interference powers outlined in part 6, chapter 3 of the Bill. These powers seem to be aimed at facilitating the hacking of overseas communications data and equipment. But wherever bulk hacking is aimed it has no place in the toolbox of government authorities. Following an investigation into the Edward Snowden leaks in 2013, President Obama’s Review Group on Intelligence and Communications Technologies recommended that intelligence agencies should focus on defending rather that engaging in attacks on network and computer security.[286]

49. Part 6 Chapter 3 should be removed in its entirety from the Bill. Part 5 needs significant amendment if it is to remain.

50. Securing systems of the magnitude of those used by security agencies and industry, and effectively proposed in the IP Bill, from external hackers or the multitude of insiders who have access to these databases (850,000 including Edward Snowden in the case of the NSA), is incredibly difficult. The joint committee will be familiar with the recent TalkTalk hack compromising the personal data of 157,000 customers.[287] You may be familiar with the even more serious and potentially life threatening compromise of the systems of US government’s Office of Personnel Management.[288] The complete dossiers of tens of millions of US federal employees, their families and others who had applied for government jobs were stolen.

[286] Richard A. Clarke, Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein, Peter Swire [13 December 2013] Liberty and Security in a Changing World: Report and Recommendations of The President’s Review Group on Intelligence and Communications Technologies
[287] http://www.bbc.co.uk/news/business-34743185
[288] https://www.opm.gov/cybersecurity/cybersecurity-incidents/

51. When you create large and valuable databases they attract attackers. Whereas, in addition to respecting data protection principles, minimising the collection and processing of personal data to that required for the specified purpose, is also good security practice.

52. Security experts like Ross Anderson, Bruce Schneier, Peter Neumann and others have written extensively about this. And to understand the problem of securing these systems you need to think about how such systems can fail - how they fail naturally, through technical problems and errors (a universal problem with computers), and how they can be made to fail by attackers (insiders and outsiders) with malign intentions. And sometimes, like the case of Edward Snowden, one of 850,000 security cleared people with access to NSA secrets, those insiders or outsiders may have, what they believe to be, benign intent. Snowden's stated intention was to disclose unconstitutional and/or illegal government agency practices. Whatever an attacker's intent, no information to which nearly a million people have access, as a routine part of their job, is secure.

53. The mood amongst western governments has been leaning towards deliberate mandates to undermine communications infrastructure security, providing security vulnerabilities for law enforcement and intelligence services to exploit. Anderson, Schneier, Neumann and other world renowned security experts recently published *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications.*[289] The paper explains, in commendably accessible detail, why this is a bad idea.

54. From their conclusion: "Even as citizens need law enforcement to protect themselves in the digital world, all policy-makers, companies, researchers, individuals, and law enforcement have an obligation to work to make our global information infrastructure more secure, trustworthy, and resilient. This report's analysis of law enforcement demands for exceptional access to private communications and data shows that such access will open doors through which criminals and malicious nation-states can attack the very individuals law enforcement seeks to defend. The costs would be substantial, the damage to innovation severe, and the consequences to economic growth difficult to predict. The costs to developed countries' soft power and to our moral authority would also be considerable. Policy-makers need to be clear-eyed in evaluating the likely costs and benefits."

Conclusion

55. The government has the right to intercept, retain and analyse personal information, when someone is suspected of a serious crime. However, current operations and the

[289] https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf

powers and processes proposed in the draft IP Bill involve collection of personal data indiscrimately, in bulk and without suspicion, in addition to network security decimating equipment interference. This is, in effect, mass surveillance.

56. Due process requires that surveillance of a real suspected criminal be based on much more than general, loose, and vague allegations, or on suspicion, surmise, or vague guesses. To operate the mass data collection and analysis systems proposed in the IP Bill, thereby giving the entire population less protection than a hitherto genuine suspected criminal, based on a standard of reasonable suspicion, is indefensible.

57. 250 years ago, Lord Chief Justice Camden decided that government agents are not allowed to break your door down and ransack your house and papers in an effort to find some evidence to incriminate you (the case of Entick v Carrington (1765) 19 Howell's State Trials 1029, 2 Wils 275, 95 ER 807, Court of Common Pleas).
58. The good judge also declared personal papers to be one's "dearest property". It is not unreasonable to suspect he might view personal data likewise in the internet age. I understand Lord Camden's reasoning in Entick became the inspiration behind the 4th Amendment to the US Constitution which offers protection from unreasonable searches and seizures. The 4th Amendment itself underpins the 46 recommendations of the Report of President Obama's Review Group on Intelligence and Communications Technologies. For a quarter of a millennium, fishing expeditions, of the type that are proposed in the IP Bill but at a scale and scope which Lord Chief Justice Camden could barely have imagined, have been considered to fundamentally undermine the rule of law. It's time Parliament brought these modern costly, ineffective and damaging surveillance practices into line with that rule of law rather than, as with the IP Bill, attempting to shape the law to facilitate and expand them in scale and scope.

18 December 2015

COSLA—written evidence (IPB0042)

1. COSLA is the main representative body of Scottish local government. We strive to operate on a consensual and cross party basis and it is in that context that we make this response to the call for evidence.

2. As we have previously stressed to Government local authority access to communications data is vital in ensuring that criminal investigations into serious matters such as illegal money lending, doorstep crime and intellectual property offences can be progressed and brought to a successful conclusion. Local authorities do not make a large number of applications for communications data and the small number of applications that are rejected shows that, when they do so, it is in a proprtionate and appropriate manner. Not only do these types of investigations prevent further harm to some of the most vulnerable in society, they also ensure that legitimate businesses can operate on a level playing field thus supporting economic growth.

3. With more and more criminal behaviour facilitated by, or conducted over, the internet or mobile telephones, it is vital that councils are able, when absolutely deemed necessary, to access communications data in order to tackle this. Councils have a key role in tackling cybercrime through their trading standards work. They use this information to build criminal cases against individuals accused of criminality, so communications data may be used to identify the person owning an email or internet address or telephone number linked to criminal activity. The increasing use of social media sites and online auction sites to sell counterfeit and illicit goods has meant that investigators face new challenges in identifying and investigating these types of crimes.

4. The introduction of judicial review of applications and the use of the National Anti-Fraud Network has introduced very rigorous oversight of the acquisition of communications data and arguably the result is that some local authorities are reluctant to use this very useful tool when investigating serious offences. The additional step in Scotland of requiring a solicitor to complete the application process to the judiciary can cause administrative difficulties for enforcement officers. The ability to streamline this process through using entirely electronic means and/or single points of contact within the legal system would be welcomed.

5. The creation of a single body to oversee investigatory powers is welcomed.

6. In conclusion COSLA strongly supports local authorities continuing to access communications data and would welcome opportunities to simplify and streamline the application process.

18 December 2015

Mr Simon Cramp—written evidence (IPB0024)

1. I want to respond to this important consultation and very large and no bars hold draft bill

2. But first some background about me

3. I have disleysic and dyspraxia and that is part of my learning differculty and in that it means I struggle to get my sentences in order but why do I mention this because my verbal reasons is ok , but I do also worry that those of us with a learning difficulty or learning disability if they carnt read or struggle with understanding what happening in terms of people are taking too fast or will there be support within the system and to help possible people with the disability understand and be able to instruct if they have a mental capacity issues . I also wonder who will police this.

4. I have lived with disability all my life and others have I have responded to other select committee in the past. I also have been a past member of the older and disabled people advisory committee for Ofcom for 7 years so I declare that interest between 2004 to 2011

5. What I like to do is perhaps make general comments in the wider overall document of the draft bill

6. The draft bill looks very good but in some areas of the draft bill explatory notes are woeful for example

7. On physic hospitals it a one sentence so general it meaningless to the average person who is not a lawyer and around the other issues of wireless act it is again explanatory notes to the average person is breath-taking rubbish with one sentence is not good enough description for such an important bill

8. I hope you find this useful

17th December 2015

Criminal Cases Review Commission—written evidence (IPB0031)

Background

1. The Criminal Cases Review Commission ("the Commission") is an independent non-departmental public body established under the Criminal Appeal Act ("CAA") 1995 to review suspected miscarriages of justice in England, Wales and Northern Ireland. If the Commission considers that there is a real possibility that the appropriate appellate court would quash a conviction or sentence, it may refer a case back to that court for a further appeal.

2. When reviewing cases the Commission is often required to carry out a certain amount of investigation. The nature, extent and depth of these investigations vary from case to case. In order to assist the Commission in the exercise of its functions, Parliament provided it with wide ranging statutory powers of investigation, most notably the power to obtain any material from any public body under s.17 CAA 1995.

3. In addition, the Commission is currently able to access communications data for the purpose of "assist[ing] investigations into alleged miscarriages of justice" under Part I of the Regulation of Investigatory Powers Act ("RIPA") 2000.[290] The draft Investigatory Powers Bill ("the draft Bill") would replicate the current position, allowing the Commission to access communications data for that same purpose.

4. The Commission has used its current powers to obtain data which have then formed the basis of a referral. For example, in July 2014, the Commission referred the conviction of Mr A to the Court of Appeal. He was convicted of rape following a trial in July 2010 and sentenced to 6 ½ years' imprisonment. The Commission obtained new mobile phone evidence, including some using its powers under Part I of RIPA 2000, which supported Mr A's version of events and were relevant to the issues of consent and the credibility of the complainant.

5. The Commission is grateful for the opportunity to provide evidence to the Joint Committee. Having considered the call for evidence the Commission has concluded that the Committee would be best assisted by the Commission limiting its responses to the areas which directly impact upon the Commission, its powers (i.e. those in relation to communications data) and functions.

Overarching / thematic questions

Are the powers sought necessary?

6. The identification, investigation and, ultimately, correction of miscarriages of justice by an independent and effective body is an essential part of the criminal justice system. The

[290] As a result of the amendments made by the Regulation of Investigatory Powers (Communications Data) (Additional Functions and Amendment) Order 2006 SI 2006/1878 – since replaced by the Regulation of Investigatory Powers (Communications Data) (Additional Functions and Amendment) Order 2010 (SI 2010/480).

Commission considers that the power to access communications data for the purpose of investigating miscarriages of justice is necessary because:

a. Communications data now regularly appears in a large number of criminal trials. As it is capable of amounting to evidence in criminal proceedings, it can also amount to "fresh evidence" which could cast doubt on the safety of a conviction.

b. Applicants to the Commission will often raise issues relating to telecommunications evidence as part of their applications.[291]

c. During the course of a review new lines of enquiry (such as an alternative suspect or person of interest who did not feature in the original police investigation) may come to light and require investigation.

d. Where there are reasonable grounds for the Commission to investigate such matters, its facility to do so should be equivalent to that of the original investigators.

e. In the absence of an explicit power to obtain communications data the Commission would be unable to do so.[292] This would, in the Commission's opinion, lead to miscarriages of justice going unnoticed and uncorrected.

Specific Questions

Does the draft Bill allow the appropriate organisations, and people within those organisations, access to communications data?

7. The Commission is pleased that the draft Bill lists the Commission as a relevant public authority and retains the purpose of accessing communications data to assist with investigations into miscarriages of justice. This would ensure that the Commission would retain its current powers to access communications data in the exercise of its functions. As previously discussed the Commission considers that these powers are necessary in order for it to be able to effectively investigate potential miscarriages of justice.

8. The investigation and review of potential miscarriages of justice is the sole preserve of the Commission. In light of that, it would, therefore, be inappropriate for anybody other than the Commission to have to power to access communications data for such a purpose, a position reflected in the draft Bill.

[291] E.g. challenging its accuracy, alleging that it was deliberately withheld or never obtained.

[292] The Commission's powers under s.17 CAA 1995 do not currently extend to private bodies and therefore do not allow the Commission to obtain communications data. A Private Members' Bill currently before Parliament [Criminal Cases Review Commission (Information) Bill 2015-16] would, if passed, extend the Commission's powers into the private sector, theoretically giving the Commission another method by which it could obtain such data. However, the Commission considers that there would be an expectation that the powers contained in the draft Investigatory Powers Bill would be the method by which communications data should be obtained (reflecting the current position under RIPA 2000) and that, as a result, it would be inappropriate for the Commission to attempt to obtain it via CAA 1995.

9. The Commission, therefore, considers that, as regards obtaining communications data for the investigation of miscarriages of justice, the content of the draft Bill is appropriate.

Is the authorisation process for accessing communications data appropriate?

10. Under the draft Bill, an authorisation for the Commission to obtain communications data can only be granted by an Investigations Adviser. The Investigations Adviser can only grant such an authority if they are satisfied that the request is necessary and proportionate to assist investigations into miscarriages of justice. The Commission cannot access communications data for any other purpose.

11. The Commission is satisfied that the authorisation process (as applied to the Commission) is appropriate because:

    a. The role of Investigations Adviser at the Commission is held by very experienced former senior police officers.[293]

    b. The single purpose for which the Commission can access data is directly related to its key statutory function.

12. The draft Bill envisages that, in normal circumstances, the designated senior officer will be independent of the investigation or operation for which the data being sought. Whilst the Commission understands and approves of the principle behind this restriction, it does not consider that it would be workable in practice for it to comply with such a requirement.[294]

13. The Commission is therefore pleased to note that clause 47(2) and (3)(c) of the draft Bill would allow its Investigations Advisor to grant the authorisation whilst still being able to actively advise on the case. The Commission considers that this exception to the general rule in clause 47(1) is necessary in order for it (and potentially other similarly small bodies) to effectively carry out its functions.

17 December 2015

[293] This role is currently held by a former Detective Chief Superintendant (a rank somewhat higher than the "designated senior officer" for the Police).

[294] Due to its small size, the Commission currently only employs one Investigations Advisor. In any case where the Commission was considering obtaining communications data, the specialist advice of the investigations advisor would almost certainly have been sought prior to an authorisation being sought.

Crown Prosecution Service—written evidence (IPB0081)

Summary

1. The Crown Prosecution Service is writing in support of the draft Investigatory Powers Bill, which was presented to the two Houses of Parliament on 4th November 2015. We consider the Bill's provisions essential to ensure effective investigations and prosecutions in a world where technology, capability and opportunity are constantly evolving.

2. Although the draft legislation is entitled 'Investigatory Powers Bill', its utility extends beyond investigations to prosecutions. Communications data and equipment interference material can be used evidentially in criminal cases and have already often contributed to securing convictions across the full spectrum of offences – including terrorism, serious and organised crime, child sexual abuse, murder, rape, harassment and domestic abuse. It is not an exaggeration to state that without these powers our capability to prosecute in these cases would be significantly reduced.

3. Communications data in particular is an essential form of evidence currently provided for under the Data Retention and Investigatory Powers Act 2014. It has played a significant role in every Security Service counter-terrorism operation over the last decade and is used in 95% of serious and organised crime prosecutions. We need to ensure that the existing powers are retained once DRIPA sunsets at the end of 2016. It is also vital that our capability keeps pace with technological advancements and the evolving practices of criminals.

4. Evidence acquired through Equipment Interference warrants will similarly be admissible in court and therefore valuable to prosecutions. This capability will enable prosecutors to acquire crucial evidence which otherwise may not be obtainable via other means. Presently such material is obtained by a combination of property interference and surveillance warrants (often alongside an interception warrant). The Bill will bring these provisions together into one place.

5. It is vital that these capabilities are maintained and modernised in order to sustain public confidence in those tasked with maintaining law, order and security in our country, in additional to ensuring that the administration of justice is fairly served. In this sense the draft Bill matters as much to the Crown Prosecution Service as it does to the Police, the National Crime Agency and the Security and Intelligence Agencies.

6. The CPS also recognises the necessity for stringent oversight, transparency and rigorous safeguards. As the RUSI review pointed out, the very fact some of this material is admissible as evidence means that it is open to full judicial scrutiny and must therefore be collected lawfully. It is also important to note that as well as helping us to identify, investigate and prosecute criminals, these powers can also help to exonerate the innocent. In keeping with our Criminal Procedure and Investigations Act 1996 (CPIA) disclosure obligations, any unused material which could undermine the prosecution case or assist the defence must be disclosed.

7. Below we have provided responses to each of the Committee's questions in turn, except for where we do not feel there is relevance for the CPS or where other parts of Government would be better placed to comment. We are happy to provide any further information if requested by the Committee.

Overarching/Thematic Questions

Are the powers sought necessary?

8. Yes. Obtaining digital information is crucial in cases which involve offending committed online (such as viewing indecent images of children), and it is also increasingly important for a wide range of more 'traditional' criminal offences (such as murder, burglary, fraud, child sexual abuse, coercive and controlling behaviour and harassment) where a phone or computer has been involved or there is a social networking or other internet link. Locating, preserving and then obtaining digital evidence is increasingly important for a whole range of criminal investigations and prosecutions.

9. Communications data in particular is an essential form of evidence used in prosecutions across the full spectrum of criminal offences. It can be adduced as part of a criminal trial. It is important that this capability is maintained and modernised, to ensure that we can keep pace as communication increasingly takes place through the internet and smart-phone apps.

Case Study: Mashudur Choudhury (Special Crime and Counter-Terrorism Division)

- **Case type:** Terrorism
- **When:** 2014
- **Details:** Choudhury was one of six men who travelled to Syria in October 2013 for the purposes of attending a training camp. He returned shortly afterwards.
- **Evidence:**
  - Most of the evidence presented relied on the content of communications retrieved from seized devices, but communications data established contact with a phone linked to Ifthekar Jaman, who had travelled to Syria earlier in 2013.
- **Outcome:** Choudhury was found guilty of engaging in conduct in preparation for an act of terrorism following trial, and sentenced to four years in prison.

10. As well as preserving our existing capability to acquire and use communications data, we feel there is a strong case for extension to include Internet Connection Records (ICRs). As we explain in the communications data section below, these will also be valuable in investigations and prosecutions across the full spectrum of offences.

Are the powers sought legal?

11. We will comment on the non-interception based powers in the Bill because these are most relevant to the work of the CPS. In our view these powers are legal. As the RUSI review pointed out, the very fact such material is admissible in a criminal court means that it is open to full judicial scrutiny and must therefore be collected lawfully:

> "Unlike much of the intelligence gained by the SIAs under Part I of RIPA 2000, evidence secured by law-enforcement agencies other than by interception is admissible in court. This subjects the intelligence to due legal process as admissible evidence and therefore the law-enforcement agency must ensure the evidence has been accessed lawfully – and meets the conditions of necessity and proportionality – for the Crown Prosecution Service to be able to bring a case and, subsequently, secure a conviction. If the evidence does not hold up to scrutiny there is a risk of the case collapsing or not making it to trial in the first place. The law of evidence – the procedures that govern proof of fact in legal proceedings – can act as a powerful constraint on law-enforcement agency actions, thereby acting as a check on law-enforcement surveillance." (4.45)

12. The law governing disclosure of unused prosecution material also helps ensure the legality of evidence. Through the proper, fair and thorough application of the Criminal Procedure and Investigations Act 1996, CPS prosecutors review authorisations and, where necessary, disclose to the defence any material that would support an argument that evidence was unlawfully obtained (and indeed any material that could undermine the prosecution case or assist the defence). In organised crime and counter-terrorism cases it is specialist prosecutors working closely with investigators who undertake this exercise.

13. We consider the legality of DRIPA later in this document.

Case Study: Operation Sable 2 (CPS Eastern Area)

- **Case type:** Witness intimidation and attempting to pervert the course of justice.
- **Details:** The defendants attempted to prevent a prosecution witness attending trial to give evidence against the OCG in a drugs conspiracy case. They went to the witness' office armed with a knife and threw a grenade at his home.
- **Evidence:**
  - Phone attribution and cell siting to identify defendants.
  - Call data to establish hierarchy of defendants and relative culpability.
  - Cell siting to identify level of participation and presence at scene.
- **Outcome:** Five defendants were convicted and each received custodial sentences in excess of ten years. The ringleader received 18 years consecutive to the 10 years he was serving for the original drugs offences.

14. As in any situation where professional privilege applies, the CPS believes that it is important that the use of investigatory powers respects the doctrine as far as possible. This is not an issue unique to communications data or the areas covered by the Bill and we manage professional privilege material responsibly and in accordance with the law in relation to all of our work.

15. We note and agree with the proposal that communications data requests intended to identify journalistic sources will attract additional safeguards beyond authorisation at official level; the relevant Code of Practice will require authorities to seek judicial authorisation. This requirement is being placed on a statutory footing as part of the Bill.

16. The privilege attached to the contents of communications between lawyer and client will similarly continue to be safeguarded. The Codes of Practice which will sit under the Investigatory Powers Bill will be consistent and at least as robust as they are at present.

Are the powers sought workable and carefully defined?

17. We believe so from a prosecution perspective, although others will be better placed to comment in relation to law enforcement and operational workability,

Are the powers sought sufficiently supervised?

18. The CPS recognises and welcomes the necessity for stringent oversight, transparency and rigorous safeguards, and believes that these conditions are met in the draft Bill. However, we believe other parts of Government will be better placed to comment on the specifics of the proposed authorisation process.

General

To what extent is it necessary for (a) the security and intelligence agencies and (b) law enforcement to have access to the investigatory powers such as those contained in the Draft Investigatory Powers Bill?

19. The CPS believes there is a clear case for the necessity of these powers for both the SIA and law enforcement. They play a crucial role in ensuring the identification, prosecution and conviction of criminals across the full range of offences. They are necessary to build stronger cases, or exculpate individuals, where otherwise there would be risks to individuals or national security if we could not prosecute.

20. Communications data in particular has played a significant role in the investigation of a large number of serious and widely reported crimes, including for example the murder of Nicholas Robinson which was the subject of a Channel 4 documentary titled *The Murder Detectives* broadcast between 30th November and 2nd December 2015. Communications data is an essential means of determining association and locational proximity with a crime.

Case Study: Operation BARDELL (CPS South West Area)

- **Case type:** Murder, conspiracy to purchase a firearm, assisting an offender.
- **When:** 2014
- **Details:** Luchiano Barnes murdered Nicholas Robinson in a dispute involving conspiracy to purchase a firearm by Barnes. Barnes had provided money to Robinson for the firearm but no weapon was supplied. Barnes subsequently fled the UK with the support of friends and family members, but was arrested after later returning to the UK voluntarily. The investigation was filmed and was the subject of a Channel 4 documentary shown on 30th November - 2nd December 2015, titled *The Murder Detectives*.
- **Evidence:**
    - Communications data was used to detail the precursor events that led to the murder, including showing the communication and travel to Bradford by Barnes, Robinson and their associates in relation to the conspiracy to purchase a firearm.
    - Communications data was also important in showing the sharp increase in communication between those accused of assisting the suspect post-incident. Alongside this the internet browsing on the handset of one of those implicated in assisting the offender allowed the investigation to show that she had knowledge of the incident before it was released in the media.
- **Outcome:** Seven defendants were convicted of a range of offences and all given custodial sentences. Barnes will serve a minimum of 23 years for murder.

Are there any additional investigatory powers that security and intelligence services or law enforcement should have which are not included in the Bill?

21. The CPS is not best placed to comment on this.

Are the new offences proposed in the draft Bill necessary? Are the suggested punishments appropriate?

22. We believe the new offences are both necessary and justified. The unlawful acquisition or disclosure of communications data constitutes a serious breach of an individual's rights.

23. Whilst the maximum penalties will be set out in statute, it is important to remember that a judge sitting in a criminal case has discretion within those parameters when handing down a sentence to anyone found guilty. The judge would take consideration of both aggravating and mitigating circumstances.

Interception

24. As material obtained by interception will continue to be excluded from legal proceedings, we feel this section is most relevant for law enforcement and SIA colleagues. The exclusion of such material extends to the prohibition of even mentioning or alluding to the existence of interception-related conduct (with some limited exceptions).Any material of this nature of which the prosecution is made aware and which may undermine the case or assist the defence would in theory be disclosable. However, the prosecution is precluded from disclosing information about such material, so in the absence of finding a judicially acceptable solution, this would lead to the case being dropped.

25. It will continue to be a criminal offence to make an unauthorised disclosure relating to interception material or activities, as is currently the case under RIPA.

Communications Data

Case Study: Operation VOICER (Organised Crime Division - Birmingham)

- **Case type:** Thirty serious sexual offences against children.
- **When:** 2015
- **Details:** Seven defendants were part of an organised paedophile network which arranged the rape of a baby, a toddler and a young child. The group sometimes drugged their victims and streamed the abuse on the dark net and Skype. They groomed a pregnant woman in order to secure access to her baby once born. The NCA said the offences were 'as vile and depraved' as it had encountered. The investigation involved the NCA, four police forces, nine local authority child protection teams, Europol and the CPS.
- **Evidence:**
    - Cell siting was used to track the use of offenders' phones at relevant locations at key times. So even though, for example, Matthew Stansfield destroyed digital evidence, we were still able to link his movement from near Portsmouth to the scenes of the crimes
    - We were able to prove Christopher Knight made several trips from Manchester to Luton to commit offending in a short time window before returning home.
    - There were also flurries of texts and calls between the offenders in the days leading up to their meet-ups, when a window of opportunity had been identified to take advantage of unsupervised children.
- **Outcome:** Two of the defendants were found guilty after trial at Bristol Crown Court; the other five had earlier admitted the various offences. They were sentenced to a total of 107 years in prison.

How well does the current process under Mutual Legal Assistance Treaties (MLATs) work for the acquisition of communications data? What will be the effect of the extra-territorial application of the provisions on communications data in the draft Bill?

26. Letters of Request (LoRs) sent as part of Mutual Legal Assistance Treaties are the means by which we obtain admissible evidence from overseas-based CSPs when coercive powers are involved. The process works but is not fast: the MLAT system takes twelve months on average to secure evidence. This is often a significant factor in delaying decisions to charge offenders or commencing a trial.

27. The UK Liaison Prosecutor in Washington D.C. handles requests to US-based CSPs on behalf of all England, Wales and Northern Ireland prosecutorial agencies. They also liaise with the US Department of Justice over any complex issues (such as ensuring Freedom of Speech is not infringed) before a LoR is formally sent. Forty-six LoRs have been executed[295] since October 2014; a further twenty-three CPS LoRs have currently been referred by the Office of International Affairs to a Federal US Attorney and are awaiting execution, and nineteen CPS LoRs are awaiting referral to a Federal US Attorney.

[295] 'Executed' means the request has been completed and evidence received by the UK Central Authority (the coordination body for all international evidence requests).

28. The length of time the LoR process takes is a source of frustration (as noted by David Anderson QC) and we are doing everything possible to speed it up:

    - The Liaison Prosecutor has daily communications with the Department of Justice to ensure that priority and urgent matters are expedited.

    - The DoJ has also recently introduced a specific team at the Office of International Affairs to help address CSP LoRs from around the world, following an increase in budget. This will result in more LoRs being executed in Washington D.C. rather than California.

29. However, there are other means of acquiring non-content information, for example when CSPs voluntarily disclose basic subscriber information when served with the UK equivalent (section 22(4) RIPA Request) of a U.S. administrative subpoena.

30. The extra-territorial application of powers to acquire communications data is important to ensure that we can continue to have access to material which is relevant to crimes committed in or relating to the UK.

Are the definitions of content and communications data (including the distinction between 'entities' and 'events') sufficiently clear and practical for the purposes of accessing such data?

31. We believe the new definitions are both sufficiently clear and viable. The draft Bill makes a helpful contribution to clarifying what is currently a complex area.

Does the draft Bill allow the appropriate organisations, and people within those organisations, access to communications data?

32. Yes, we believe it does.

Are there sufficient operational justifications for accessing communications data in bulk?

33. This is primarily a question for investigative partners, as bulk communications data is not frequently used in prosecutions.

Is the authorisation process for accessing communications data appropriate?

34. Authorisations for obtaining communications data are different to interception or equipment interference warrants. While Secretary of State or Judicial Commissioner approval is not required, the CPS considers that the authorisation process is nevertheless robust, effective and independent: it is a proportionate regime given that the communications data in question does not include the actual content of any such communications.

<u>Data Retention</u>

Do the proposed authorisation regime and safeguards for bulk data retention meet the requirements set out in the CJEU *Digital Rights Ireland* and the Court of Appeal *Davis* judgments?

35. The Government was given permission to appeal the ruling of the Divisional Court in the *Davis* JR, and the Court of Appeal judgment was handed down on 20th November 2015. The Court of Appeal considered that it was not clear that EU law had laid down definitive mandatory requirements in relation to retained communications data and reached the provisional view, contrary to the view of the Divisional Court, that EU law did not have that effect. The Court of Appeal referred questions on the effect of EU law to the Court of Justice of the European Union. The Government welcomes the judgment of the Court of the Appeal. The case is ongoing.

Is accessing Internet Connection Records essential for the purposes of IP resolution and identifying of persons of interest? Are there alternative mechanisms? Are the proposed safeguards on accessing Internet Connection Records data appropriate?

36. This is primarily a question for law enforcement colleagues to answer, although the benefits of the contribution ICRs could make in enabling investigators to identify suspects are evident. If law enforcement colleagues are unable to identify suspects then we cannot prosecute them. This includes for cases of child sexual abuse or online exploitation, where LE partners have articulated a compelling argument for how ICRs would make a significant difference to our collective ability to tackle offending. Furthermore, because ICR information could be used evidentially, this would also contribute to securing convictions which at present simply are not possible due to lack of evidence.

37. We are confident that the sensitive nature of ICRs is reflected in the proposed safeguards in place, including the limitations on who can apply to access them.

Are the requirements placed on service providers necessary and feasible?

38. There are other, more technically-focused, organisations that will be better placed to answer this question than the CPS. However, we always strive to minimise our requirements on CSPs and are appreciative of the assistance they provide to us.

<u>Equipment Interference</u>

Should the security and intelligence services have access to powers to undertake (a) targeted and (b) bulk equipment interference? Should law enforcement also have access to such powers?

39. We would answer in the affirmative to the questions above. Evidence acquired through targeted Equipment Interference warrants will also be admissible in court and therefore valuable to prosecutions. This capability will enable prosecutors to obtain crucial evidence which otherwise may not be available. Presently such material is obtained by a

combination of property interference and surveillance warrants (often alongside an interception warrant).

40. Material collected under an EI warrant can be used evidentially but in practice it rarely is at present. The only recent example we are aware of concerns the case of John and Ann Darwin, whose email communications were obtained with the use of a property interference warrant. EI is primarily used as an investigative capability, and any evidence retrieved from, for example, a personal laptop or phone can usually be later acquired during examination of the exhibit (using the Police and Criminal Evidence Act 1984) following the arrest of the suspect.

Case Study: Ann and John Darwin – the 'missing canoeist' (CPS North East Area)

- **Case type:** Seventeen offences relating to deception and money laundering.
- **When:** 2009
- **Details:** The case of John and Ann Darwin attracted widespread media attention following Mr Darwin's apparent disappearance in a canoe at sea. It was subsequently alleged that Mr Darwin had faked his own death to enable his wife and he to make a new life for themselves in Panama on the proceeds of insurance payouts. A total of $973,248 was transferred out the UK. He pleaded guilty but his wife denied the charges with a marital coercion defence.
- **Evidence:** Emails between the husband and wife – while he was in Panama and she in England – were obtained via property interference and surveillance warrants and adduced at trial. The prosecution was able to demonstrate conclusively that there was conspiracy to defraud and that Ann Darwin was a willing associate rather than the victim of coercion from her husband.
- **Outcome:** Both defendants were convicted and given custodial sentences.

The Equipment Interference power will remove the current requirement to combine property interference and surveillance warrants to obtain evidential material from equipment, as happened in this case.

Are the authorisation processes for such equipment interference activities appropriate?

41. The CPS believes so.

Are the safeguards for such activities sufficient?

42. The CPS believes so.

Bulk Personal Data

Is the use of bulk personal datasets by the security and intelligence services appropriate? Are the safeguards sufficient for the retention and access of potentially highly sensitive data?

43. Although there is nothing in the Bill which prohibits the evidential use of bulk personal data, in practice it is most often used as an investigative tool to identify targets. Only the Security Service, the Secret Intelligence Service and GCHQ are authorised to collect bulk personal data and as a result it is most appropriate for them rather than us to answer this question.

Oversight

44. Other parts of Government will be better placed than the CPS to respond on this section. However, we would reiterate the point that material which is going to be adduced as part of a criminal trial will by definition need to be legal – in the sense of being lawfully obtained – otherwise it would be thrown out by a trial judge. This proposal therefore effectively provides an additional layer of judicial oversight. The CPS welcomes any oversight arrangements which make the collection of evidence more robust and able to withstand challenge in court.

Alison Saunders
Director of Public Prosecutions, Crown Prosecution Service
December 2015

21 December 2015

Cryptomathic Ltd—written evidence (IPB0115)

Background

This note is written on behalf of a software company in security, and I am the founder and executive chairman, former professor of mathematics. We are a software company that delivers security servers for banks, large enterprises and government, always based on encryption techniques.

What we produce in a nutshell

These servers are typically used for generation of cryptograms for the generation of debit- and credit cards, e-passports, for electronic banking, legally binding digital signatures and large scale encryption of transactions and confidential business data. Thus we have delivered the servers for all British e-passports, and we have some of the large banks in the UK and the rest of the world as our customers.
Common to almost all these solutions is that the actual encryption takes place in a so-called hardware security module (HSM), which is tamper resistant, i.e. the encryption keys are extremely difficult if not impossible to recover. These modules are typically produced by large vendors, e.g. in the UK (Thales e-security), USA (Safenet, Atalla) and Germany (Utimaco)

Hardware Security Modules and their importance

These HSMs are sold without export restrictions to most countries e.g. in Europe and USA. The way they are currently built, there is no so-called trapdoor that would allow anybody to supply the encryption key e.g. to law enforcement authorities. You may for certain applications include a trapdoor in programmable HSMs, which apply to some on the market, but you could not do that without revealing it to the end-customer, as they would require the source code for security reasons.

The Problem with the proposed legislation

We just wanted to raise a serious alert and point out that if authorities were to enforce British HSM vendors to include a general hardware trapdoor –or even might potentially enforce this with the coming legislation in hand - this would likely be devastating to British HSM vendors, as banks and others all over the world would then likely switch to non-British vendors to be on the safe site – just as they would not even consider to use Chinese HSMs.

Strong encryption is impossible to prevent anayway

On a more general note, I would like to point out that it is just as difficult to prevent someone capable of general programming who sets his mind on applying strong encryption from doing so, as it is to prevent e.g. terrorists and hardcore criminals from using deadly weapons.

This note has been kept short on purpose, but I am happy to elaborate if need be.

21 December 2015

Simon Davies—written evidence (IPB0121)

Summary

1. This submission addresses the Committee`s primary question about the justification for new security legislation and new powers. I argue that purported evidence for the new law is highly unstable and could result in increased public risk and decreased public trust in national security. I submit that the procedural framework to test assertions in support of the measures is out of date and wholly inadequate. This submission also previews the findings of a major international consultation by Code Red on alternative, integrated models for assessing security legislation.

About me

2. I have been a specialist and an advocate for privacy for almost thirty years. During that time I founded numerous organisations and initiatives, including Privacy International. I have advised a large number of organisations, including the United Nations High Commission on Refugees and the British Medical Association, along with numerous professional, corporate and government bodies. For sixteen years I lectured in privacy and data protection at the London School of Economics, where I still serve as Associate Director of LSE Enterprise. In recent times I founded a new non-profit privacy initiative called Code Red,[296] which brings together many of the world1s leading policy experts, journalists, technology developers and whistleblowers.

The context for this submission

3. This submission addresses the Committee`s first question, namely, *has the case been made for both the new powers and for the restated and clarified existing powers.* As such, I will not offer detailed comment on the technical, ethical and legal aspects of the Bill. Those elements have been thoroughly analysed by many of my colleagues and their views have already been expressed to the Parliament.

4. The reasoning at the heart of this submission peels back the Committee`s primary question and argues that it may presently not be possible to deploy a rational framework to accurately justify the new powers. While there exists a considerable body of *data* relating to aspects of the Bill, the question I will discuss here is whether this data constitutes a true foundation of evidence to adequately protect public safety and privacy. I will propose a solution that the Committee may wish to consider.

5. For the sake of clarity, this submission assumes that everyone contributing to the legislative process – regardless of their view of the Bill – wants the UK to build effective and workable security systems. Such consensus cannot, unfortunately, be

[296] https://codered.is/

claimed for privacy. Many people in the security realm continue to believe that privacy and security are opposing elements. I agree with many of my colleagues that strong operational security does not need to come at the expense of strong privacy. The experience, for example, of the National Security Agency`s *ThinThread* and *Trailblazer* surveillance programs demonstrated that it is possible to establish protective measures that respect individual rights while creating a robust and accountable security framework (e.g. *ThinThread*). Conversely, a poorly designed security framework (e.g. *Trailblazer*) will compromise both privacy rights and security. I would argue that – under the present rationale - key measures in the IP Bill fall largely into the latter category.

6. In saying this, I am not arguing that the Bill`s contentious measures can be "tweaked" into acceptability. My colleagues have already advised that some key elements of the Bill are fundamentally flawed. I would go a step further by arguing that many of the Bill`s cure underlying assumptions are fundamentally flawed. This shortcoming, I believe, is a matter that should be of vital concern to the Committee.

7. I am not alleging that Parliament has erred in respecting the established *process* for the passage of this Bill. My argument is that any measure that proclaims to genuinely protect public safety in the modern age should be subjected to a higher and more integrated test than might apply to other legislative areas. The existing organic process is simply not good enough.

8. In order to maintain both public trust and public safety, any claim to the need for increased surveillance and state power must be tested by way of a transparent and robust evidence-based framework. This task is squarely within Parliament`s domain.

Background to this submission

9. In 2014 – following a global surge in security and policing legislation – Code Red (an independent advocacy organisation of which I am co-director) engaged an international consultation process to identify trends in security legislation and the extent of integrity of the claims being made to justify those measures. Meetings were conducted in eleven countries, hosted by such organisations as *Amnesty International* (Denmark and Germany), *the University of Amsterdam Institute for Information Law, European Digital Rights* and *Nätverkstan* in Gotenborg.

10. These "Integrity Project" meetings identified the following core negative characteristics of security legislation over the past fifteen years:

> *Countries throughout the world have adopted laws that expand the power of police and security agencies – often at the expense of privacy and individual rights. It has been argued that many of these measures are untested, unnecessary and disproportionate, and some - such as large elements of US bulk metadata collection - have been largely discredited.*

Public support for these control and surveillance measures – often created at times of 'heightened risk' – have frequently been fuelled by irrational, false and populist beliefs and assertions.

Only on rare occasions have such laws been based on a solid foundation of evidence. Importantly, even fewer have been subjected to any form of structured risk assessment. In some cases, such legislation is fuelled by rhetoric, rather than reason.

The specific elements of security legislation have not been built "from the ground up" but have been cherry-picked through a process of policy laundering. That is, countries tend to adopt measures that have already achieved critical mass at an international level. That critical mass is instinctively judged as evidence for their need and - by default - becomes "conventional wisdom" and thus, self-evident.

As a result, privacy incursions are now so ingrained into the legal and technological fabric that mass surveillance and wide-scale intrusion are part of the genetic structure of security operations.

While nearly all legislative proposals have been subjected to some form of structured process (legal advice, human rights compliance, public hearings etc.), in all cases there have been substantial deficiencies in this process. These are itemised later.

The arguments put forward by security agencies have tended to be anecdotal in nature. These anecdotes serve as powerful tools to inspire support for new powers, but their veracity and relevance is rarely – if ever – independently assessed prior to legislative drafting.

11. The almost five hundred people who attended the Code Red consultation meetings were asked to consider which elements and questions they would like to see added into the legislative framework. The most common responses were as follows:

    Has a full risk assessment been conducted on potential negative or risky consequences of the proposed legislation?

    To what extent have other approaches been considered? Has an options paper been produced in advance of the draft law?

    Have any independent expert parties been formally engaged to assess the viability and integrity of the proposals?

    Has the international experience been structurally assessed in terms of outcomes from similar proposals?

    Has a clear and transparent evidential framework been developed to prove the necessity of the proposals?

12. It was rightly argued that parliamentary committees do serve some of these functions. However – as the Committee doubtless knows all too well – security legislation is frequently subjected to a tight time frame, and there is little opportunity to reflect on such foundation elements. Clearly, an accountable and comprehensive process needs to be embedded into the very design of draft legislation.

13. Participants overwhelmingly expressed concern about the justification for new security powers. The overriding view was that a means must be found to test such claims and to ensure that they are not spurious, emotive or inflammatory. Amongst the most prominent categories identified were:

    Claims about the overall security threat to communities;

    Claims about security trends at the national and international level;

    Vague or inflammatory language used to sell security legislation;

    Claims about the potential benefit of increased security powers;

    Claims about the effectiveness of security measures in other jurisdictions;

    Assertions about the current effectiveness of security and policing agencies;

    Assumptions about the "negative" effects of strong data protection on effective security;

    Assertions about the need for collection of greater volumes of communications and other data:

    Assertions about the need for increased secrecy in security operations.

14. Most of these points are present in the gestation of the UK IP Bill.

15. As the Committee will be aware from other evidence, the assertions made by security agencies are frequently at stark variance with those made by some independent experts. The very basis of some technical assumptions for the Bill have been roundly condemned. The viability of bulk collection too has been challenged globally. That this polemic has arisen so late in the Bill`s gestation is regrettable – and unnecessary. An integrated evidence framework would anticipate such conflicts and identify the full range of options.

Research resources

16. Code Red`s findings are fundamentally supported by a raft of recent research at the international level. This includes:
    a. *The University of Amsterdam: "Ten standards for oversight and transparency of national intelligence agencies", the Institute for Information Law.*[297]
    b. *The Council of Europe; "The rule of law on the Internet and in the wider digital world", Douwe Korff.*[298]
    c. *European Fundamental Rights Agency; "Surveillance by intelligence services: fundamental rights safeguards and remedies in the European Union - Mapping Member States' legal frameworks".*[299]

17. This literature, together with reports from the likes of the EU Parliament`s LIBE Committee, highlight the urgency of a more robust approach to regulation of communications and the Internet.

21 December 2015

Dr Andrew Defty—written evidence (IPB0050)

1. This submission deals primarily with the question of whether the powers set out in the draft bill are **sufficiently supervised,** and focuses in particular on interception by the intelligence and security agencies. It also offers some comments on the issue of **protections for MPs' communications** and the status of the so-called 'Wilson Doctrine'.

2. The submission draws upon the findings of a major research project on parliamentary scrutiny of the intelligence and security agencies carried out by a team of researchers at the University of Lincoln, which has been published in a number of journal articles and a book.[300] This submission also reflects comments made in a submission to the Investigatory Powers Review conducted by David Anderson, QC. The research on which the submission it based was funded in part by the Leverhulme Trust and examined the various mechanisms by which parliament and parliamentarians seek to scrutinise the intelligence and security agencies, including through legislation, debates, the work of the Intelligence and Security Committee and other parliamentary committees and the tabling of questions and motions. In addition to a detailed examination of parliamentary business (reports, debates, EDMs and questions), the research drew on interviews with more than 100 MPs and Peers, including four former Home Secretaries, six former Foreign Secretaries, current and former members of the Intelligence and Security Committee, and with senior officials in the Foreign Office and the Cabinet Office. This submission also draws upon some follow-up research on the impact of recent reforms on the operation of the parliamentary Intelligence and Security Committee.

[297] http://www.ivir.nl/publicaties/download/1591
[298] http://www.coe.int/t/dghl/standardsetting/media/cdmsi/Rule_of_Law_Internet_Digital_World.pdf
[299] http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services_en.pdf
[300] H. Bochel, A. Defty and J. Kirkpatrick, *Watching the Watchers: Parliament and the Intelligence Services*, London: Palgrave, 2014.

Nature of the oversight framework

3. Intelligence oversight is generally defined as a process of supervision designed to ensure that intelligence agencies do not break the law or abuse the rights of individuals at home or abroad. It also ensures that agencies are managed efficiently, and that money is spent properly and wisely. There is, however, no one model of oversight. It does, of necessity, vary from country to country, and may be affected and defined by a state's history, constitutional and legal systems, and political culture. Nevertheless, it is possible to identify a range of institutions and actors that may be involved in the oversight of intelligence and security agencies. Oversight is typically seen as taking place at several different levels: internal oversight at the level of the agency; executive oversight by the government; legislative oversight by democratically elected politicians, usually through specialist legislative oversight committees; external oversight by independent bodies such as the judiciary; and oversight by civil society through actors such as pressure groups and the media.

4. Britain has a patchwork of oversight arrangements involving different actors with different roles. This multi-faceted approach has a number of advantages. A combination of organisational and functional oversight serves to overcome the potential accountability gaps when oversight arrangements are tied to specific agencies. A combination of Executive and legislative scrutiny is an important check on legislative power, and the use of external review processes involving judges, not only helps to ensure that covert activities are carried out within the law, but may also serve to lift oversight above political partisanship. However, there are also a number of potential problems with what may be seen as a patchwork approach. It is important to ensure that as changes take place, both organisationally and functionally, that oversight mechanisms are adapted to keep pace with change and gaps do not emerge. It is also important to remember that each level of oversight has a distinct and important role in terms of providing effective and credible oversight and that changes in the role and powers at one level do not compensate for deficiencies at another level. For example, in the context of the draft Bill changes to the authorisation process do not obviate the need for strong *post hoc* review. In considering reform of any aspect of the regulatory framework consideration should be given to the framework as a whole to ensure that accountability gaps do not emerge.

The authorisation process for the issue warrants

5. The draft Bill restates the principle that warrants for interception by the intelligence and security agencies are issued by a Secretary of State. The involvement of Ministers at this point is important in terms of maintaining democratic accountability and legitimacy. In our research we interviewed a number of those with direct experience of the warranting procedure, including former Home and Foreign Secretaries. These individuals testified as to the robustness of the warranting process, the seriousness with which they approached the task and the amount of time they devoted to reviewing every warrant. However, the existing warranting process does raise a number of concerns. It is anomalous that warrants for the interception of communications and covert intrusion,

actions which involve the state in the most serious intrusion of individual liberties, are signed by a Government Minister and not a judge. Moreover, given the large number of warrants signed each year there are also obvious concerns about the amount of time available to a busy Secretary of State to scrutinise each warrant in detail. In our submission to David Anderson's review we recommended that an additional layer of independent judicial scrutiny at the point at which warrants are signed may help to relieve the burden on hard–pressed Ministers and also provide more effective scrutiny of the process. **The draft bill's inclusion of a 'double-lock procedure whereby warrants issued by a Secretary of State would require approval by a Judicial Commissioner before coming into force is a significant improvement on the current arrangements.**

6. The main potential point of contention would appear to be the stipulation, at section 19 (2), that in approving a warrant, Judicial Commissioners must apply the same principles as would be applied in cases of judicial review. This reflects the recommendations of the RUSI report but not those of the Anderson review. I am not convinced that this represents a significant limitation on the powers of the Judicial Commissioner, particularly when considered alongside section 19 (1). Moreover, judges have consistently shown themselves prepared to exercise considerable rigour and independence in the application of judicial review in other, related, areas such as control orders. Lord Pannick's recent article in *The Times* was particularly convincing in this respect.[301] However**,** the advantages are of this limitation on the role of Judicial Commissioners are not clear. **If a Secretary of State is convinced of the case for interception, as they always claims to be, and particularly when a process exists to challenge the decision of a Judicial Commissioner, then allowing Judicial Commissioners to review the application on the same terms as Ministers would seem to provide a more robust system and one which is less open to criticism.**

7. In my view a more significant flaw in the proposed authorisation procedure is the mechanism whereby Ministers might appeal against the decision of a Judicial Commissioner. Section 19 (5) states that where a Judicial Commissioner refuses to approve a decision to issue a warrant, the decision may be referred to the Investigatory Powers Commissioner. The authority of the Investigatory Powers Commissioner to approve warrants is set out in section 167 (6), which states that the Investigatory Powers Commissioner will be a Judicial Commissioner. **Allowing the Investigatory Powers Commissioner to act as final approval in the issue of warrants represents an undesirable blurring of the roles of authorisation and oversight.** It is the role of a Judicial Commissioner to approve the issue of warrants, while the role of the Investigatory Powers Commissioner is to provide *post hoc* review of this process. The draft Bill makes the Investigatory Powers Commissioner the ultimate authority in decisions about the issue of warrants, whilst also being responsible for reviewing such decisions. It should go without saying that it is not a good idea for those responsible for making decisions, to also be responsible for reviewing their own decisions. While it might be beneficial for the post of Investigatory Powers Commissioner to be held by an individual who has previously served as a Judicial Commissioner, the two roles should not be combined. **If a process for challenging the decision of a Judicial Commissioner is**

[301] D. Pannick, QC 'Safeguards provide a fair balance on surveillance powers', *The Times*, 12 November 2015.

to be included in the Bill then the model set out in the Anderson report whereby one of the Judicial Commissioners would be designated as the Chief Judicial Commissioner would be preferable to involving the Investigatory Powers Commissioner in the authorisation process.

8. One long-standing area of ambiguity which is not clarified in the draft Bill relates to which Secretary of State is responsible for signing interception warrants. The field of intelligence is one in which few parliamentarians, or indeed government Ministers, have any experience and the application of investigatory powers as set out in the Bill is complex. It is standard practice that Home Office warrants are signed by the Home Secretary while warrants for covert activities abroad are signed by the Foreign Secretary, while those relating to defence intelligence may be signed by the Secretary of State for Defence. However, neither in previous legislation or the draft Bill is it specified which Secretary of State should sign warrants, or who should sign in the absence of the relevant Secretary of State. While it is clear that in most cases warrants will be issued by a Secretary of State with the appropriate knowledge and understanding of the process, this may not always be the case. As part of our research we interviewed a former Secretary of State from a different department entirely, with no experience in this area who claimed to have routinely signed Home Office warrants when the Home Secretary was unavailable. **In order to ensure that the arrangements for issuing warrants is robust it would be helpful if the Bill specified in more detail which Secretary of State should issue warrants and what the process should be in the absence of the designated Secretary of State. It would be preferable if, in the absence of the designated individual, a clear chain of responsibility was established which involved passing warrants to another designated Secretary of State or upwards to the Prime Minister, rather than to a Secretary of State from any other department.**

The Investigatory Powers Commission

9. The draft Bill includes significant proposals for reform of the current independent oversight regime, most notably with the establishment of a new and powerful Investigatory Powers Commission. **The creation of a single Investigatory Powers Commission to replace the patchwork of existing commissioners is a welcome development.**

10. The new Investigatory Powers Commission is likely to be a powerful body but there is a need to ensure that it does not overlap with other oversight bodies. As noted in paragraph 7 above, **it is important that the role of the Investigatory Powers Commission, which is one of audit, inspection and review, is kept separate from that of the Judicial Commissioners who are directly involved in authorisation.** There is also potential for some overlap between the work of the Investigatory Powers Commission and the parliamentary Intelligence and Security Committee. In addition to overseeing the warranting process the draft Bill provides the Commission with a wide remit, which includes, at the Prime Minister's request, keeping under review 'any aspect of the functions of' the intelligence services, the heads of the intelligence services and the any part of the armed forces engaged in intelligence activities. Not only does this expansive

role place an extra burden on the resources of the Commission, it also appears to overlap considerably with the functions of the Intelligence and Security Committee. The lack of clarity about roles can, of course, lead to duplication but may also lead to accountability gaps if each body assumes that the other has primary responsibility in a particular area or case. There is also the possibility that governments can play scrutiny bodies off against each other, assigning tasks to the body which it assumes will offer the most agreeable response, or when duplication occurs being able to pick and choose which findings to accept. **While ensuring close cooperation between the various oversight bodies, it would nevertheless be beneficial if a clear demarcation was maintained between their respective roles, and in particular if some clarity was provided in relation to the overlapping statutory roles of the Investigatory Powers Commission and the parliamentary Intelligence and Security Committee.**

11. The main challenge involved in establishing this new oversight body is to ensure that sufficient resources are made available. The Investigatory Powers Commission will be replacing at least six existing offices (section 178 (1)), while this will inevitably serve to prevent some duplication, it is important to ensure that the creation of the new body should not lead to any loss of function or capacity. There can be a tendency to view resources allocated to oversight as detracting from those which might be devoted to the important work of protecting national security. However, as noted in paragraph 3 above, oversight is not simply about ensuring that intelligence agencies do not exceed their powers, it is also an important means of maintaining and improving effectiveness. Efficacy and oversight are not mutually exclusive, and rigorous and effective oversight should be seen as a force multiplier when it comes to combating threats to national security. While it is difficult to legislate for sufficient resources, **it is nevertheless, crucially important to ensure that the new Investigatory Powers Commission has sufficient resources in terms of staffing, budgets and expertise. In particular, it is vital that it has the necessary technical expertise in order to effectively exercise its functions.**

Additional protection for Members of Parliament and other legislatures

12. The draft Bill includes new protections for the communications of Members of Parliament and other legislative bodies (section 16). To date the interception of the communications of parliamentarians has been covered by the Wilson Doctrine, a convention established by the Prime Minister, Harold Wilson, in 1966. Successive Prime Ministers, including the current one, have expressed their continued commitment to the application of the Wilson Doctrine and the convention continues to have strong support amongst parliamentarians. However, there is also considerable confusion, in parliament and beyond, about the scope of the Wilson Doctrine[302] and it has come under pressure in recent years, notably from the Interception of Communications Commissioner who called for its repeal and from the Investigatory Powers Tribunal which concluded that it had no legal basis. **The passage of legislation relating to the interception of communications since the 1980s means that the Wilson Doctrine is now out of step**

[302] A. Defty, H. Bochel & J. Kirkpatrick, 'Tapping the telephones of Members of Parliament: the Wilson Doctrine and Parliamentary Privilege' *Intelligence & National Security*, vol.29, no.5 (2014), pp.675-697.

with the current statutory framework. If parliament believes that the communications of parliamentarians should be treated differently to those of other members of the public then the draft Bill provides a clear opportunity to place the Wilson Doctrine on a statutory footing.

13. One notable anomaly of the Wilson Doctrine, which has become more obvious in recent years, is that it has only been applied to members of the House of Commons and the House of Lords. **The draft Bill's extension of additional protections to members of the devolved assemblies and UK members of the European Parliament, in addition to members of the Westminster Parliament, serves to resolve a notable inconsistency in the current operation of the Wilson Doctrine.**

14. However, while the protections set out in the draft Bill do represent a raising of the bar when it comes to the interception of communications of members of the relevant legislatures, **in its current format the Bill does not represent a codification of the Wilson Doctrine**. The Wilson Doctrine comprises two elements. The first is a general, although not absolute, prohibition on the interception of communications of Members of Parliament by the intelligence services. The second is that, if there is a change in that general policy the Prime Minister will inform Parliament, at a time commensurate with the interests of national security. The proposed protections in the draft Bill arguably enshrine the first element, but there is no provision for the second. **If it was felt desirable to codify the Wilson Doctrine more fully, one possible solution could be a process whereby the Prime Minister will inform the parliamentary Intelligence and Security Committee, or possibly the committee's Chair, if a warrant is issued for the interception of the communications of a member of a relevant legislature.**

Conclusions and Recommendations

The authorisation process for the issue warrants

A. The draft bill's inclusion of a 'double-lock procedure whereby warrants issued by a Secretary of State would require approval by a Judicial Commissioner before coming into force is a significant improvement on the current arrangements.

B. If a Secretary of State is convinced of the case for interception, as they always claims to be, and particularly when a process exists to challenge the decision of a Judicial Commissioner, then allowing Judicial Commissioners to review the application on the same terms as Ministers would seem to provide a more robust system and one which is less open to criticism.

C. Allowing the Investigatory Powers Commissioner to act as final approval in the issue of warrants represents an undesirable blurring of the roles of authorisation and oversight. If a process for challenging the decision of a Judicial Commissioner is to be included in the Bill then the model set out in the Anderson report whereby one of the Judicial Commissioners would be designated as the Chief Judicial Commissioner would be

preferable to involving the Investigatory Powers Commissioner in the authorisation process.

D. In order to ensure that the arrangements for issuing warrants is robust it would be helpful if the Bill specified in more detail which Secretary of State should issue warrants and what the process should be in the absence of the designated Secretary of State. It would be preferable if, in the absence of the designated individual, a clear chain of responsibility was established which involved passing warrants to another designated Secretary of State or upwards to the Prime Minister, rather than to a Secretary of State from any other department.

The Investigatory Powers Commission

E. The creation of a single Investigatory Powers Commission to replace the patchwork of existing commissioners is a welcome development.

F. It is important that the role of the Investigatory Powers Commission, which is one of audit, inspection and review, is kept separate from that of the Judicial Commissioners who are directly involved in authorisation.

G. While ensuring close cooperation between the various oversight bodies, it would nevertheless be beneficial if a clear demarcation was maintained between their respective roles, and in particular if some clarity was provided in relation to the overlapping statutory roles of the Investigatory Powers Commission and the parliamentary Intelligence and Security Committee.

H. It is crucially important to ensure that the new Investigatory Powers Commission has sufficient resources in terms of staffing, budgets and expertise. In particular, it is vital that it has the necessary technical expertise in order to effectively exercise its functions.

Additional protection for Members of Parliament and other legislatures

I. The passage of legislation relating to the interception of communications since the 1980s means that the Wilson Doctrine is now out of step with the current statutory framework. If parliament believes that the communications of parliamentarians should be treated differently to those of other members of the public then the draft Bill provides a clear opportunity to place the Wilson Doctrine on a statutory footing.

J. The draft Bill's extension of additional protections to members of the devolved assemblies and UK members of the European Parliament, in addition to members of the Westminster Parliament, serves to resolve a notable inconsistency in the current operation of the Wilson Doctrine.

K. While the protections set out in the draft Bill do represent a raising of the bar when it comes to the interception of communications of members of the relevant legislatures, in its current format the Bill does not represent a codification of the Wilson Doctrine

L. If it was felt desirable to codify the Wilson Doctrine more fully, one possible solution could be a process whereby the Prime Minister will inform the parliamentary Intelligence and Security Committee, or possibly the committee's Chair, if a warrant is issued for the interception of the communications of a member of a relevant legislature.

18 December 2015

Digital–Trust CIC—written evidence (IPB0117)

1 This submission, dated 21st December 2015, is from Digital-Trust CIC. In summary we hope to explore whether the Bill:

- Adequately consolidates the position reached by RIPA, its amendments and whichever subsequent case law expresses Parliament's original intentions, as well as consolidating various 'creatively interpreted' surveillance measures only recently made public.
- Resolves any of the still-outstanding lacunae in RIPA.
- Accurately and transparently express the Home Office's stated policy objectives.
- Have any unintended consequences, particularly ones that would have a chilling effect on investigations into crimes such as Stalking and Harassment which fall outside the "Serious, Organised" umbrella.
- Unacceptably dilutes the privacy rights of ordinary law-abiding members of the public, in other words is seen to be proportionate and necessary.
- Properly delivers technology neutrality.
- Avoids the perception pitfalls of RIPA – such as the 'Terrorism' vs 'Poole Council' effect, and any overly obscure drafting which dilutes public confidence that the Bill is indeed as transparent as claimed.
- Does it in fact make unauthorised investigations ("snooping" even) by members of the public as illegal as unauthorised investigations by law enforcement.

2 There are bound to be places where we have accidentally misinterpreted the Bill, or previous legislation, or the Home Office's declared policy objectives; for which we apologise in advance, but the submission below is based on our current understanding of such matters. We also apologise that within the necessarily short timescale available, and length of submission expected, that the text might be quite dense and be missing several hyperlinks to citations which in a more perfect world we would have provided.

3 Digital-Trust CIC campaigns for greater clarity in the law with regard to digital crime and abuse, to better protect victims and make it easier for the police and relevant victim-supporting NGOs to understand what tools they have at their disposal. The potential consolidation of more than sixty earlier statutes, as recommended in the Anderson Report, is something we wholeheartedly support.

4 This submission based on one of Digital-Trust CIC directors, Roland Perry's, experience of drafting significant amendments to RIPA, plus his membership of the Internet Crime Forum's Data Retention subgroup and editor of the ensuing report, his oral evidence to the Joint Scrutiny Committee for the draft Communications Bill (eg Paragraph 357 of the second volume of the 2002 report of the Joint Scrutiny Committee), input on Internet issues to the original accredited-SPOC training course, to the first RIPA codes of practice, attendance as the sole ISP representative in the early 2000's at the ACPO precursor to the National Police Chiefs' Council Comms Data Working Group , as industry vice chair of the Internet Crime Forum, and from developing and delivering training to all the first cadre of NHTCU recruits in Internet Governance ecosystem and Open Source investigative methods.

5 More recently, we have written guides on securing mobile phones and minimising their online footprint, mainly to combat harassment of victims by other individuals. We have also been monitoring public and press reaction to the draft IP-Bill, and have attended all of the first six oral evidence sessions of the committee.

6 Digital-Trust CIC also offers training and advice regarding digital abuse to criminal justice agencies and charities such as Women's Aid and the National Stalking Helpline, and their directors were responsible for the national guidelines on Stalking and Harassment: Digital Stalking - A guide to Technology Risk for Victims. We are also the secretariat for the Digital Crime APPG.

History

7 Before IOCA 1985, interception was permitted by s45, Telecoms Act 1984, and before that had no statutory basis. After IOCA came into force, s45 was amended to refer only to acts of disclosure, rather than the interception itself, and post-RIPA has been repealed completely.

8 As we understand it, the OIC is of the opinion that any organisation running a virus checker or a spam filter is conducting Interception. The third party in this case might be a machine doing the profiling in order to perform the detection or gather statistics on the number of such emails in circulation.

9 It's unlikely that the sender of such emails would consent to the process, thus that exception can't apply. Is it a better public policy objective that infected or spam emails be deleted, and thus not available to either the network administrators or the intended recipient, rather than being quarantined for both parties (only one of whom is the intended recipient) to review later?

10 Interestingly we have gone full circle, from the original telecommunications statutes apply to telegraph matters, and only later revised to include voice, and now we are still in the process of adding all forms of "contact services" onto a framework based on a model of voice communication.

11 Shorthands used by us in this submission

Agency - Any public authority mentioned in Bill, including Security Services, police, local authorities and other investigating authorities.
"Contact Services" - To clarify when "Telecommunications Service" used in the Bill is a Skype/Twitter/email "over the top" service which would NOT qualify under RIPA 12(4)(b) as being "incidental"; rather than a telecommunications conveyance service such as Vodafone or O2, or a site that would qualify under RIPA s12(4)(b) which we can therefore call a "media-delivery site" - trying hard to avoid the already pre-defined word "content".
All references to "clauses" are clauses in the draft IP-Bill.
Reference to "emails" refer to all forms of content including, but not limited to, pager messages, voicemail, SMS and instant messages.

Our position

12 Firstly, because they are often referred to as the only changes in capability being sought in the IP-Bill, we observe that the questions of "What is an ICR" and "how intrusive are they intended to be" are still lacking sufficient clarity, despite (or because of) numerous conflicting interpretations of that rather short part of the Bill, of the Explanatory Notes, and associated briefing documents, being aired in oral evidence and elsewhere.

13 Taking a slightly different approach to normal (we are aware that the wording in the Draft Bill as un-amended may not reflect exactly what the Home Office originally intended) we are still trying to decide if the wording in 193(6) is intended to apply to ICRs, or is it only applicable to the Communications Data in 193(5), and hence the IP-Bill's version of the "up to the first slash" drafting in the tailpiece of RIPA s21(6)(d). Where is the prohibition in the definition of ICRs in clause 47(6) which would then rely upon the definition of content in clause 193(5). And where is the definition of "internet service" as used in clause 47(4)(a).

14 Law enforcement has given oral evidence that they read 47(4)(b) as only allowing access to information about "Contact sites" [see our unofficial definition above]. The explanatory notes mention bbc.co.uk which is clearly **NOT** a "Contact site", Facebook.com which clearly **IS**, but Google offers both types of service including Gmail and Groups **within** the "Contact site" definition, and Search and Maps within the **NON-**"Contact site" realm. In addition, the expression "Web browsing" is extraordinarily non-neutral. Is a Facebook App or Twitter app on a smartphone, as opposed to their view-it-in-an-Internet-Explorer-browser version, "browsing"? Is "browsing" limited to sites using the http protocol, or does it also extend to other protocols in rfc1630, page 11, such as ftp?

15 On the grounds that it's the **retention** of ICRs which facilitates the required extra capability, then the Home Office's stated policy objective of not storing web browsing records is not fully delivered because they would be storing partially redacted web browsing records. On the other hand the definition of what the IP-Bill requires to be retained, in 71(9)(f), appears to revert straight back to RIPA s21(6), but without the tailpiece. However, that tailpiece's main function is to redact the RIPA Traffic Data to something as relatively less intrusive as "The IP address of the apparatus hosting the bbc.co.uk website". Or perhaps "the apparatus hosting redacted.bbc.co.uk" because news.bbc.co.uk and sport.bbc.co.uk could easily be on two different apparatus, but the scheme isn't supposed to reveal that degree of detail. Other problems arise if bbc.co.uk is hosted on the same apparatus as topgear.com, in that scenario which reverse-DNS result is the CSP supposed to log? Or what if bbc.co.uk is hosted on multiple load-balanced machines, or topgear.com is on the same cloud-services site as other unrelated programmes such as strictlycomedancinglive.com

16 We fully understand that knowing that someone is using a particular 'internet service' is sufficient, because enquires can then be made of that service provider, or of relevant other ICRs having ascertained the service being used. Some commentators worry that their phone might be chatting away to Twitter automatically in the small hours, but that's irrelevant if what the agencies want to discover is that they have an active Twitter account. If you want to know 'when' and 'from where' they actually posted to Twitter, there are Open Source

tools to help discover that, or ask Twitter. We don't think it's realistic to expect the agencies to polls all of the trendy-social-media-sites-this-week, to see if someone has an account there, although there are some new "big data" aggregating sites which are getting close to being able to answer such a query.

17 Perhaps not enough attention has been paid to the fact that many users will have several access providers and swap between them at different times of day according to which appliances they are using, or where they are. The author is quite capable of using a broadband connection at home, mobile data from at least two phone companies en-route, Virgin's wifi on the tube, Abellio's wifi on the train, and the Palace of Westminster's in-house public wifi, all within the space of a few hours. That's a lot of people who have to keep records that one day someone may have to correlate. And we are also an ex-customer, over the period of a year, of several additional paid-for access services, let alone the many free ones such as the complimentary wifi at Heathrow Terminal three.

18 There's also the issue, not resolved in RIPA, which relates to one-to-many communications. If an email is sent to members@mailinglist.com , who is the intended recipient – the email server which replicates the message to hundreds of members, or the hundreds of members themselves. This has implications if you wish to legally intercept the communications based on the consent of the recipient(s).

19 The final missing piece in the jigsaw is references in circulation about ICRs being able to allow agencies to determine that for example a travel agent's site has been visited, and thus allow them make focussed enquiries. That's the best bit of evidence that the "Contact-site" (versus "Media-delivery site") restriction so often mentioned, doesn't in fact exist.

Content, or not

20 One other area where we think greater clarity would perhaps lay some fears to rest is the "actuation" provisions in clause 193(2)(b). This is much the same as RIPA 21(6)(c) and was introduced there at a very late date to enable the police to record the tones used to perpetrate "dial-through" fraud on certain PABXs. It was felt that because the tones were audible, they might have been regarded as content (of the call to the PABX), whereas in fact they are much more akin to the situation where callers to large institutions are often greeted with the message "if you know the extension number you want, dial it now". There is a contrary view, however, that the role of such tones fall within the normal definitions of Comms Data if you consider the ensuing end-to-end communication, once the second hop has been established.

21 It's possible, but we are aware of many case studies, to interpret this section "creatively" and come up with other situations where something which would normally be regarded as content is reclassified as traffic data. A possible example would be an email server set up to notice the word "Urgent" in the title, and send a designated recipient a text to warn them to go look at their email. At which point perhaps all subject lines of emails might not be "content".

22 We have in the past programmed an email server to look at a line in (some) email headers which says how many subsequent lines the email has, and then split those pending emails into "short" and "long" in two different mailboxes, so the former can be collected unencumbered by the latter, if on very limited bandwidth connectivity such as a GPRS phone (rather than a 3G).

23 It is possible that some rumours that an email containing a phone number is allowed to be 'intercepted' using the comms data provisions in order to extract that phone number, but we have not yet been able to confirm from exactly which clause that fear arises.

24 Phone numbers themselves can be tantamount to content if there's just one purpose for calling it. From http://www.theaa.com/travelwatch/roadwatch.jsp it's clear that a landline dialling 0906 88 84322 is someone enquiring about road traffic information, and in fact grabbing the next few tones will tell an investigator which motorway or road they might be thinking of using. Dialling 123 is equivalent to "tell me the time" and http://www.eif.co.uk probably means a person is thinking of visiting Edinburgh in August. More study is required before we can conclude how these various matters might be dealt with under clause 193(6).

25 Ignorance of jargon is no excuse – RIPA introduced many new concepts, which CSPs did eventually comprehend and were therefore able to implement in measures when eventually requested. See the discussion in paragraph 20 of "activation of apparatus". There also appears to be a misconception amongst smaller CSPs that one day they will receive a notice out of the blue and have to start wondering what it means and what they will have to do to comply. We are confident that almost all notices will only be issued after a significant amount of pre-consultation with the CSPs, and an agreement on costs has been reached.

26 But that does remind us of the provisions in RIPA for agencies to self-authorise to gather comms data for themselves, if faced with a clueless CSP. Accessing the logs of a PABX at a hotel being the classic case study used during the passage of RIPA. We haven't yet looked at how that aspect has been transferred across to the IP-Bill.

Suggestions for possible improvements:

27 It should be possible to renew, on demand, the retention period for individuals under investigation – if that's technically feasible. There has been discussion of the need to retain data in order to provide it to the defence if someone files an alibi defence at a late stage. It's our understanding the current form of caution "it may harm your defence if you do not mention when questioned something which you later rely on in court" is largely aimed at warning suspects that late-arriving alibis are a bad idea.

28 We understand that one of the policy objectives of RIPA was to stop the practice of gathering emails using PACE orders, although the test case concerning NTL in 2001 sided with Suffolk Constabulary, and was upheld on Judicial Review.

29The provisions inherited from RIPA 1(5)(c) and appearing as clause 5(1)(c) were originally intended to mitigate the unintended consequence that legitimate seizing of a computer containing emails might be construed as Interception, but perhaps should be revisited to

ensure that if the only thing being seized are undelivered emails then an Interception warrant should be sought. The explanatory notes for RIPA make a good case for previously delivered emails being accessible this way, but not such a strong one for yet-to-be-delivered ones.

30 More clarity is required on the circumstances where altering the routing rules on (eg) a cloud-based system comprises an illegal interception. And whether it matters (it should) whether it's done with or without the account-holder's permission. Emails sent to one of our email addresses is delivered in the conventional way to both a desktop/laptop, plus a second copy to Gmail, who then forward a second copy to our smartphone, with the original sitting as webmail in the cloud.

31 It should be an interception offence (rather than merely Computer Misuse) for someone to "hack" into either of the servers where the copying is taking place, and either specifying additional copies or interfering with the copies currently being made, or of course reading the webmail. For now we are going to assume that interception warrants and/or equipment interference covers the activities of the agencies in this regard. For clarity, the policy in clause 3(4)(b) should also be applied to the definition of "in the course of its transmission", in clause 3(1).

32 The Home Office has asserted that offences under the Bill will apply equally to agencies and members of the public. But clause 8(2) restricts the offence of unlawfully obtaining communications data to persons within the agencies.

33 Similarly, the exemption in 2(2) for unlawful interception on a private network is too widely drafted, although we are aware it's copied from RIPA s1(6).

34 Sadly, too many of today's very connected households contain bad actors and it should be an offence to "snoop" in those circumstances, although this could be implemented by adding a subclause referring to persons who had expressly withheld their consent.

35 If you are the person controlling the wifi in a house, there's no operational need to intercept it. On the other hand, conduct by the operators of public telecommunications systems such as is permitted by RIPA s3(3) does not appear to be reflected in clause 2.

36 It might, however, be possible to argue that all users of public telecommunications systems, should they also be included in 2(2), have given implied consent to the operator to intercept their communications for operational purposes. To what extent that consent is wisely given to all operators of free public wifi on private premises, is another question.

Transparency and public confidence.

37 The Bill still has drafting incomprehensible to the layperson, which reduces public confidence; "Data includes any information which is not data" - cf things like "any data identifying the data or other data as data comprised in or attached to a particular communication" in RIPA.

38 It would be preferable to split ICRs into three elements (like we successfully lobbied for in a previous life, regarding RIPA Comms Data) – and perhaps introduce a specific reference to further subdividing the powers to use clause 47(4)(c) ICR data type between different agencies.

39 It would be useful if the public were better informed about the number of subjects under investigation by interception warrants, viz the number of fresh warrants issued each year; rather than the number of fresh, renewed and modified warrants lumped together. A similar clustering of the statistics relating to requests for Comms Data might reduce the shock of seeing six-figure numbers in the Commissioner's reports.

40 Perhaps considering changing the urgent-warranting delay two working days not five calendar days (which is a standard figure in data retention legislation to cope with events at 6pm on Maundy Thursday not being noticed until 9am on the following Tuesday) would more accurately reflect the operational realities.

41 Commissioners should have technical capability in-house because very many of the data leaks on "New Media" are a result of unforeseen consequences of access to one thing revealing another. A trivial example would be the access to photos with geo-tagging by default, surprising the photographers by revealing where the photos were taken.
42 We welcome the merging of commissioners, and recommend they are appointed for a renewable five year period, mindful that many would not seek reappointment. We also support BT's oral evidence that the ICO's responsibilities in this area should also be transferred to the unitary Comissioner's office.

43 We also welcome the extension of the remit of the TAB and the reinforcement of the role of SPOCs.

44 Much of the bad publicity, and subsequent lack of public confidence in, RIPA is along the lines of "we were told it was justified because of terrorism, but now it's being used by the Egg Marketing Board to catch farmers counterfeiting Lion stamps, or local authorities wanting to poke around in our recycling bins or check we aren't committing school catchment area fraud".

45 However, the whole range of purposes and agencies were available from the start. Once the Act was being implemented the list of agencies shrank, rather than grew (although not originally including the Scottish DEA was a potentially embarrassing oversight).

46 One of the amendments which we pioneered in a former life was to split the original draft definition of comms data into three ascendingly intrusive categories, with a view to public confidence being improved if it was possible for not-every-agency to be given one-size-fits all powers.

47 One of the issues we have yet to study sufficiently, is whether the new clause 193 categories of Entity Data, Events Data and the rump of Comms Data adequately reflect that strategy. As with any of the other matters discussed in this submission, we would be happy to expand on any matters of interest to the Committee.

48 In conclusion, we would recommend considering using the same strategy to split the three forms of ICR disclosure in clause 47(4) into separate named categories (eg IP Address resolution, Identifying Internet Services, and tracing the flow of Illegal material).

49 The latter might, for example be restricted to CEOP's operations, whereas IP Address Resolution is not especially intrusive, and merely restores capability back to where it was before the introduction of Carrier Grade NAT.

50 A similar process back in the pre-RIPA days of dial-up Internet was introduced to enable the traceability of the multiple subscribers who adopted, in turn, the IP address of their ISP's modem to which they were assigned. While the ISP may have had one telephone number with a hunt-group with many individual modems on "extensions", each of those modems potentially a pool of thousands, would have a unique IP address and logs held (or perhaps not initially held by default) could determine who was authenticated to each modem at any particular time/date in the past.

51 We have recently conducted some tests of mobile-phone CGN, and contrary to the evidence given to the committee we have observed the same IP address being assigned to multiple connections over a period of hours or days. But the port number may have changed.

Further Work

52 We have not yet had the time to study in detail how the Bill addresses many issues not explicitly mentioned above, including the International aspect, the day to day mechanisms for oversight and the issuing of authorisations, nor anything to do with filtering or bulk warrants, or the estimated costs to CSPs of implementing the Bill.

53 We do, however, agree with some witnesses that the smaller the CSP, an investment of a greater proportion of their annual turnover would be required to comply.

54 There's also the issue of whether blocking a communication based on a view taken of its content as infected by a virus or Spam, is interception (the unintended recipient being the wastebin).

55 And we've seen comments to the effect that definitions of "telecommunications systems" should be more properly aligned with EU Directive and Communications Act language, rather than inherited from rather old Telecoms Act definitions.

56 We have not yet come to a view whether data retained as ICRs is available to a subject access request (and therefore potentially infringe privacy between family members). Potentially this would expose "Ashley Madison" users to the person in whose name the broadband is delivered to the house.

57 We aren't sure who will be responsible for ICRs in an MVNO situation (the physical carrier or the virtual carrier). Or how the tracing required by the Bill would apply to already

existing “over the top” services from major telcos, such as ‘Wifi calling’, let alone hitherto unhead-of services from start-ups launched during the possibly ten year period the resulting Act is in force.

21 December 2015

Jamie Dowling—written evidence (IPB0149)

1. My name is Jamie Dowling. I am a London based IT professional with over 15 years' experience in the IT sector covering all aspects of service and technical support. I am also a campaigner against abuses of privacy and Due Process.

2. Historical Context:

    2.1. The mass surveillance measures proposed by this Bill will slaughter the right to personal privacy that the United Nations holds that everyone should have. The European Court holds that mass surveillance of any population is illegal.

    2.2. The internet is a powerful tool which enables communications and sharing of information like never before. Those who choose to be better informed about things which affect their lives now know more about those things and are much better placed to engage with them. This includes politics, healthcare and civil liberties to name but three.

    2.3. The ability to collate and store information about citizens' day to day lives, movements and communications (the term "communications data" has not been specifically defined) is a concept that would have appealed massively to those in repressive states such as Nazi Germany, the USSR and East Germany. Ethically this Bill places the Prime Minister and Home Secretary above Heydrich, Stalin and Honecker. Indeed the Prime Minister uses phrases like "terrorist sympathisers" to describe those who would ask simple direct questions about air strikes on Syria; such language befits those named previously.

3. Question: Are The Powers Sought Necessary?

    3.1. The powers sought are being sought via a flawed belief that mass surveillance works. It does not. The Madrid bombings would not have been stopped by mandatory ID cards and mass surveillance, neither would the 7/7 bombings. There is no substitution for proper detective work with proper intelligence gathering. Mass surveillance is lazy and by its nature bound to be inaccurate. Government would do better if it stopped blaming Edward Snowden and put resources into proper detective work.

4. Question: Are The Powers Sought Legal?

    4.1. Simply put, no they are not. Mass surveillance is illegal. This judgement is held by both the Court of Justice Of The European Union and the European Court of Human Rights.

5. Question: Are the powers sought workable and carefully defined?

5.1. No they are not. What constitutes an “internet connection record” has yet to be clearly and accurately defined. Government thinking is clearly pie in the sky; major telecoms companies have told Government that the Bill is "so technically complex that it is not yet possible to make any meaningful estimate of the costs involved or whether they are technically possible."

5.2. Adrian Kennard’s evidence to Government clearly shows that it literally does not understand how the Internet works. In that context nothing has changed from one of my earlier submissions to Government, the 2009 APCOMMS committee where I recommended that Government appoint an independent committee of technical experts to advise on its ideas for internet policy. That suggestion was ignore and this latest attempt to bring in a Snooper's Charter is not just dangerous, misguided and fundamentally unworkable.

5.3. No Bill can ever be considered “futureproof”. Where we are now could never have been envisaged by politicians and governments 15 years ago. This Bill is inadequate as it stands so by definition it cannot be considered futureproof.

6. Question: Are the powers sought sufficiently supervised?

6.1. Does the Judge actually investigate that the interception is justified? If the answer is not an unqualified “Yes” then the powers sought are not sufficiently supervised. Interceptions must only ever be authorised by a Judge after a full justification has been presented to the Judge by the Home Office.

7. Additional Comments

7.1. The distinction between "content" and "communications data" is meaningless when you haven’t clearly defined what they are in the first place. Metadata is actually more revealing than content, because it is already parsed in a computer-readable form that allows it to be combined with billions of other pieces of metadata.

7.2. Creating huge databases of metadata will create huge honeypots that will be irresistible to criminals and foreign governments. Stealing the metadata will give them valuable information that can be used for identity theft or blackmail. The Government’s refusal to publish the metadata relating to the Home Secretary is sufficient justification for asserting that opinion.

7.3. The whole idea of "equipment interference" is stupid. If agencies are given permission to break into people's systems, they can plant anything there, and make changes to things like browser histories. As a result, any computer evidence in a trial is suspect, since it could easily have been planted using "equipment interference" without anyone noticing. As computer-based evidence becomes more important, "equipment interference" would seriously undermine the UK's legal system. It should be the very rare exception, not part of a standard toolset.

8. Conclusion

8.1. Just as in 2009, Government still does not understand how the internet truly works. It is using the language of fear to try and impose a blanket surveillance regime that it cannot adequately or accurately define and which may well be technically impossible.

8.2. Many will view this Consultation and Bill simply as an attempt to legalise the illegal mass surveillance which the security services have been engaged in over the last decade. Government may try to persuade us that such databases do not exist but PRESTON and ECHELON clearly do. These surveillances have happened. These databases exist. Why? Government has tolerated illegal surveillances by the security services and by commercial companies such as Phorm. It now needs to revisit the illegal surveillances that have happened and legislate to prevent further illegal surveillances.

8.3. To try and implement the proposed regime would be a massive waste of money and resources and irretrievably damage the UK's reputation as a good place to do business. Any interception must be subject to proper judicial oversight ensuring due process and full justification. Government must rip up these fundamentally ill-considered proposals and concentrate on proper police and intelligence work rather than implement this ignorant knee-jerk shambles.

23 December 2015

Mark Dzięcielewski—written evidence (IPB0082)

1. Another Snoopers' Charter, rushed through without time for detailed scrutiny

Despite the pre-publication propaganda, the Draft Investigatory Powers Bill is *not* any simpler than RIPA and DRIPA the short timescale for the public to digest and the Joint Committee to produce a report into a 300 page Bill is clearly inadequate.

The Home Office has had literally years to come up with the wording of this Bill, so the rush to rubber stamp it into law without proper detailed scrutiny looks like an anti-democratic trick by those in power, which has **already further weakened public trust** in the whole exercise.

2. Necessary reforms to RIPA which are not included in the Draft Bill

All sections of RIPA need revising, including

2.1 Covert Human Intelligence Sources and online "Legend" building

Given the "SpyCops" scandals involving the rape of several women political activists by undercover policemen, the welcome changes to the Codes of Practice dealing with Covert Human Intelligence Sources should have been incorporated into this Draft Bill.

Given the increasing use or abuse of "online" social media identities to establish KGB style false identity "Legends" for undercover officers (the previous technique of stealing the identities of dead babies is now frowned upon) , this should also have been regulated on the face of this Draft Investigatory Powers Bill

2.2 Cryptography.

Given the current war on Cryptography by the technologically ignorant , the inadequate protections against abuse under RIPA Part III regarding cryptographic keys or forced decryption should have been revised in this Draft Bill No detailed Codes of Practice - yet again Yet again Parliament and the public are being asked to approve Enabling Legislation, without sight of the detail of any proposed detailed Statutory Codes of Practice.

3. Counterproductive secrecy for Retention Notices for Communications Data

Others have pointed out the stupidity of the ban on mentioning the existence of Interception Warrants and the banning of Intercept Evidence from UK Courts.

Why has the Home Office decided to arbitrarily add secrecy to the Communications Data Retention Notices ?

Enforcement

> 77 Enforcement of notices and certain other requirements and restrictions
>
> (1) It is the duty of a telecommunications operator on whom a requirement or restriction is imposed by—
> (a) a retention notice, or
> (b) section 74 or 75,
> to comply with the requirement or restriction.
>
> (2) A telecommunications operator, or any person employed for the purposes of the business of a telecommunications operator, must not disclose the existence and contents of a retention notice to any other person
> (3) The duty under subsection (1) or (2) is enforceable by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or for any other appropriate relief.

This stupid wording ("**any person**") means that when, not if, such Communications Data is challenged in Court, as to its validity, accuracy or completeness, there is no leeway or scope for a "Telecommunications Operator" to attest to or swear to the validity, accuracy or completeness of the Communications Data they have been forced to provide, having been served a Retention Notice, without breaking clause 77 (2)

This stupid secrecy provision must be removed from the Bill - it has not been necessary in the last 15 years under RIPA, so why bother with it now ?

The danger is that crucial Communications Data evidence cannot be used in Court or may be grounds for an appeal, because the “Telecommunications Operator” cannot swear to its validity, accuracy or completeness because of cl 77 (2)

4. Bulk Personal Datasets

4.1 Acquisition of Bulk Personal Datasets

The Joint Committee needs to probe typical Bulk Personal Dataset acquisition scenarios and make the Home Office explain in detail what the oversight and protection for innocents is in cases such as:

- Open Source from internet e.g. Ashley Madison, password dumps by hackers
- Seizure as part of evidence in an on-going criminal case,
- Voluntary hand over for free e.g. Data Protection Act request to other UK Public Authorities or private companies or individual Data Controllers.
- Handed over by Foreign Intelligence Agency partners e.g. Five Eyes USA, Australia, New Zealand, Canada or other European Union or NATO allies.

- Bought Commercially (with or without National Security discount) Swapped for other data from a Data Broker - Huge risk to UK innocents privacy & security Stolen Hacking

4.2 Protection of existing Statutory Gateways

A warrant for a Bulk Personal Dataset must *not* be used to circumvent the normal procedures for a Statutory Gateway, established clearly by an Act of Parliament to permanently link two public sector databases together

e.g. like the Department for Work and Pensions Longitudinal Study link to HMRC tax and employment records established by the Employment Act 2002 s13 Supply of information held by the Board
http://www.legislation.gov.uk/ukpga/2002/22/section/13

4.7 No "hacking" of UK Public Sector Bulk Personal Datasets

"acquisition" of Bulk Personal Datasets must never include "equipment interference" / "hacking" or the use of Covert Human Intelligence Sources aimed at UK public authorities or companies who hold some or all of the Bulk Personal Data.

e.g. Census or Medical or Tax or Welfare records or the BBC TV Licensing database one of the more accurate Name and Address registers)

4.3 Medical records must never be allowed to be grabbed as a Bulk Personal Dataset

All the recent Strategic Defence Reviews rightly treat Pandemic Infectious Diseases as a potentially far greater threat to the National Security of the United Kingdom than mere terrorism.

If even a single "Typhoid Mary" infectious carrier of a lethal infectious disease is dissuaded from seeking prompt medical help, because they fear that their Medical Records could end up in the hands of the police or intelligence agencies, then the consequences to public health could be disastrous.

There is no scenario where the acquisition of Bulk Medical Records either in the UK or overseas, can ever be proportionate, even for "national security" purposes.

4.4 Mosaic requests building up a full Bulk Personal Dataset piecemeal by stealth should be illegal

Mosaic requests building up a full Bulk Personal Dataset piecemeal by stealth should be illegal Multiple Bulk Data Set warrants must not be in force at one time

A history of Bulk Personal Dataset requests must be kept and checks made to ensure that a "mosaic" approach to grabbing a whole database, a few pieces at a time, beneath the threshold of the need for a Secretary of State warrant, is not allowed

Partial requests for less than "the majority" of data of innocents must not be allowed as a loophole to build up a copy of a whole Database without bothering to obtain an individually signed Warrant.

e.g. **All** current records in full database e.g. 100,000 records (Names A to Z) - Secretary of State signed Warrant required

But a request structured to capture **only 49%** of records in the database – still tens of thousands of records of innocent people – there is no need for a Secretary of State signed warrant

2 different or only partially overlapping requests for 49% of the databases e.g. one for records numbers 1 to 49,000 (or Names from A to M) and a second request for records 51,000 to 100,000 (or names from N to Z) must not be allowed

4.5 Treat the Bulk Personal Datasets of innocent foreigners like innocent UK citizens

Foreign based Bulk Personal Datasets e.g.

Airline Passenger Name Records

Ashley Madison adultery website data breach

Liechtenstein or Swiss Bank "tax avoider" records for sale by a whistleblower which contain less than 50% of records relating to UK citizens

must still require a Warrant and Secretary of State and Judicial Commissioner approval

4.6 No Duplication of Bulk Personal Datasets warrants signed by different Secretaries of State

The Draft Investigatory Powers Bill should be amended:

There needs to a central clearing house for the vetting of Bulk Personal Dataset requests.

There must*not*be multiple purchases of the same or almost the same Bulk Personal Dataset from a Commercial source by each of the Intelligence Agencies - this would simply be a waste of money and is likely to lead to errors and omissions amongst multiple copies of such datasets held in secret by GCHQ. SIS and MI5

There must*not*be multiple "acquisitions" of the same or almost the same Bulk Personal Dataset through the use of "hacking" or "equipment interference" by each of the Intelligence Agencies

4.8 No sale or free handover of Bulk Personal datasets to Data Brokers or Foreign Governments

There must be no sale or swap or free handover, of partial or full Bulk Personal Datasets of UK persons to commercial Data Brokers (e.g. as part of a deal to "acquire" a foreign datasets they hold or sell).

Similarly once "acquired" Bulk Personal Datasets must not be swapped or traded with Foreign Governments or agencies .

Since Bulk Personal Datasets will almost certainly include details belonging to (innocent) Foreign citizens, these must receive the same protection and audit as those of innocent UK citizens.

4.9 No "jurisdiction shopping" amongst "Five Eyes" allies regarding Bulk Personal Datasets

UK Intelligence Agencies have denied that they have mutual oversight "jurisdiction shopping" arrangements with allied "Five Eyes" foreign intelligence agencies whereby e.g. NSA spies on UK citizens to evade British scrutiny, and GCHQ spies on US citizens to sneak around US legal restrictions on spying on Americans.

This must not be allowed to happen under the currently inadequate wording of the Draft Investigatory Powers Bill with respect to Bulk Personal Datasets.

4.10 "Filter" for Bulk Personal Datasets as well as for Communications Data

Why is there a "Filter" mechanism for Communications Data requests,
but not for Bulk Personal Datasets ?

If the technology and procedures for a Communications Data Filter
exist to handle e.g. billions of mobile phone SMS message metadata
records every day, then surely smaller Bulk Personal Datasets can
also be filtered in the same way ?

4.11 Bulk Personal Datasets can be even more intrusive than Communications Data

e.g. access to the Census data on religion -
the potential basis for future harassment, ethnic cleansing or
genocide. In 1930's Germany The Nazis determined if you were a Jew
by cross referencing the ethnic / religious data from 19th century

Census records of people's grandparents.

4.12 Amend the Draft Bill to include criminal penalties for abuse of Bulk Personal Datasets

There must be a similar criminal penalty to protect partial or full Bulk Personal Datasets from abuse by officials or sub-contractors.

> 8 Offence of unlawfully obtaining communications data
>
> (1) A relevant person who knowingly or recklessly obtains communications data from a telecommunications operator or postal operator without lawful authority is guilty of an offence.

Without such a penalty, clearly on the face of the Bill, there can be no public confidence or trust in the oversight of this section of the Bill.

In order to discourage abuse of Bulk Personal Datasets by UK or foreign **Data Brokers**, who may or may not have been contacted by the UK intelligence services,, this criminal offence should also include the possibility of an **unlimited fine**.

5. IMSI catchers or Cell Site Simulators

The Joint Committee must find out about the current use of IMSI Catchers or Cell Site Simulators
https://en.wikipedia.org/wiki/IMSI-catcher
https://theintercept.com/2015/12/17/a-secret-catalogue-of-government-gear-for-spying-on-your-cellphone/
It is totally unacceptable that, currently, the Interception Of Communications Commissioner denies all responsibility for oversight of the use of such devices.
Apparently they are authorised by the Surveillance Commissioner, as if they were simple electronic bugging devices planted during a Police Act 1997 Part II "property interference".
Technologically this is nonsense, as thy work by actively jamming and intercepting the radio communications between mobile phone handsets and the real mobile phone network, by pretending to be Cell Towers to which the mobile handset will connect with.
This is clearly both **Interception** and also "**equipment interference**" i.e. "hacking". Since more than one, potentially hundreds of mobile phone handsets, could be affected, this could also be "**bulk equipment interference**"
Since modern SmartPhones are also primarily Computers, there are Computer Misuse Act Denial of Service attack implications as well (intelligence agencies have no exemption under CMA, only the police).
Even if these devices are narrowly targeted, they inevitably cause "collateral disruption" to innocent Mobile Phone voice calls and to Data streams.
In the worst cases they can **block emergency 999 calls** and thereby **put lives at risk**.

The Joint Committee must get the Home Office to explain exactly how these devices are going to be dealt with under the Draft Investigatory Powers Bill and what the oversight mechanism is.
It is not acceptable to rely on an as yet still secret Code of Practice, this must be clearly stated on the face of the Bill.

21 December 2015

EE—written evidence (IPB0139)

About EE

EE is a joint venture formed by the merger of the UK businesses of T-Mobile and Orange in 2010, and is owned in equal shares by its parent companies Deutsche Telekom AG and Orange SA (formerly known as France Telecom). EE operates the UK's fastest, largest and most reliable mobile telecommunications network with over 31 million connections across its mobile, fixed and wholesale businesses and has pioneered the introduction of 4G. We provide 2G services to over 99% of the UK population, 3G to over 98% of the population and 4G to 95% of the population, with the figure growing every week. It operates the EE, T-Mobile and Orange brands, and through its wholesale operations supports third party brands, such Virgin Mobile, which it hosts on its network as virtual network operators.

General Comments on the Draft Bill

EE welcomes the opportunity to respond to this Call for Written Evidence. EE recognises the importance of the powers set out in the Draft Bill and is committed to work with the Home Office to create a workable regime.

The existing legislative framework supporting the retention and acquisition of Communications Data (CD), the provision of Lawful Interception (LI), including the safeguarding and oversight of such, has fallen behind as technology advances and is becoming less valid in the internet age. In light of Edward Snowden's revelations, and the subsequent public concerns, together with the huge and rapid advances in technology, EE believes that the wholesale review of legislation, resulting in the publication of the Draft Investigatory Powers Bill, has been essential.

The Draft Bill raises a number of important issues and EE is keen to contribute to this debate and provide expert advice where it can. The Call for Written Evidence asks a number of specific questions; however, we will only respond to those questions that we believe are relevant to EE as a telecommunications operator. EE would like to make some general comments on the Draft Bill before this response addresses the specific questions raised in the Call for Written Evidence.

In relation to the overall purpose of the Bill, we believe we understand what the Government has set out achieve – which is to attempt to provide a clear, transparent, comprehensive and comprehensible legislative framework, pulling together the multiple fragmented pieces of communication surveillance legislation that currently exists, whilst maintaining and in some cases enhancing surveillance capabilities. The Draft Bill also provides greater oversight and safeguards.

Although EE has been provided with verbal assurances from the Home Office in relation to the scope of the Draft Bill, the Draft Bill itself is lacking crucial details that EE needs in order to assess the Bill's impact on its businesses and for all to assess its proportionality. With a rapidly changing communications environment and the transmission and storage of communications becoming more and more fragmented, we have concerns that this

legislation will place more and more responsibility and obligations upon telecommunications operator in the future. This makes it difficult for EE to assess the impact of the Draft Bill on our business and provides no protection by way of legal certainty about what lies ahead.

We are concerned that there are practical difficulties in distinguishing communications data from content data. Furthermore, it must be appreciated that any solutions to the gathering and/or generation of data may detrimentally affect the quality and speed of communications that EE can offer to their customers. In addition, the proposals may force EE to re-design its networks to meet the obligations for collection and retention at the expense of efficiency and speed. The proposals may also impact EE with regards to 'time to market' of services we are offering. If the Government fails to ensure that 'Over the Top' providers are within scope of the legislation, this may create a two tier system where telecommunications operators affected by the Bill take longer to bring a service with full facility to market relative to others.

The Home Office suggests a cost of £174m to implement the proposals but we have not been consulted and did not see how these figures have been derived. A general view from industry is that the estimated costs provided by the Home Office have yet to be fully validated and there is some concern that this figure may underestimate the actual future costs. Only once testing of capability has progressed sufficiently can more accurate costs be supplied. It is important to understand the assumptions made in estimating these costs and furthermore EE would expect to be able to recover all of its costs and not just a "reasonable contribution".

Although EE understands the need to maintain capability in order to prevent and detect crime and save lives, the new powers under the Draft Bill place increased responsibility and liability upon UK telecommunications operators. There will be increased regulatory burdens beyond current legal obligations, together with increased demands and disclosure volumes. Customer trust is central to our business. It is therefore incumbent upon the Government to do all it can to explain to the public why it feels these powers are necessary, to ensure the processes will remain robust and proper oversight will be consistently exercised, and that the security provisions we already have in place to protect customers' data can and will remain strong.

Draft Investigatory Powers Bill – Call for Written Evidence

- **Are the powers sought necessary? Has the case been made, both for the new powers and for the restated and clarified existing powers?**

The decision as to whether the case for the new powers and for the restating and clarification of existing powers is convincing is a matter for Parliament. However, there are a number of areas of the Draft Bill that require further research and assessment, not least Internet Connection Records (ICRs). Despite the Government providing use cases and justification for the retention of ICRs, there are a number of significant technical challenges

that may impact Law Enforcement and the Security and Intelligence Agencies (SIAs) achieving full benefit from this data. We hope that the evidence we provide to the Committee, together with the evidence from other key sectors, including Law Enforcement, privacy groups, civil society and academics, will assist Parliament in making this assessment.

- **Are the powers sought workable and carefully defined? Are the technological definitions accurate and meaningful (e.g. content vs communications data, internet connection records etc.)? Does the draft Bill adequately explain the types of activity that could be undertaken under these powers? Is the wording of the powers sustainable in the light of rapidly evolving technologies and user behaviours? Overall is the Bill future-proofed as it stands?**

This is an incredibly complex area, and even more complex to define within a piece of legislation. However, the definitions do provide a basis for further discussion and defining capabilities. In terms of the types of activity that could be undertaken under these powers, the Bill provides for a broad framework to require telecommunication operators to acquire, generate and retain data.

The Home Office has provided verbal assurance that there will be no requirement for EE to retain third party data. However, on the face of Bill there is very little limitation on what Government could require telecommunications operators to do. We believe that CD should only relate to data that is required by us, as a telecommunications operator, to provide a service and, in relation to Internet Protocol (IP) connections, deliver a packet of data from a sender to a recipient. CD in this instance is the information that is available and visible to us as a network in order to do this. Any data within a packet that is not processed by a telecommunications operator to provide a service to its customer is the payload that we have no need to process. This may or may or may not be content under the definitions of the Bill.

EE believes that Clause 71(9) of the Bill should be modified to give effect to the assertion that the term 'relevant communications data' should specifically relate to data generated on a telecommunications operator's own network or processed by that operator in order to provide a service (and therefore would not apply to data simply transiting the network with no activity undertaken upon it). Such wording would preclude a requirement on telecommunications operators to retain transit data.

The power to require a provider to "generate" data for the purposes of retention (S71(8)(b)) is also of concern (one that also existed with the Draft Communications Data Bill), with fears that it could be used to require a provider to generate data that does not relate to providing a service to our customers. Again, a modification of Clause 71(9) as above would preclude this requirement.

We believe that clarifying the obligation on telecommunications operators on the face of the Bill will provide both a future-proofed piece of legislation, together with greater clarity on obligations. However, RIPA was introduced 16 years ago and Government should not wait another 16 years for reviews and amendments to this legislation. More frequent reviews would allow to legislation to keep up with technology.

- **Are the new offences proposed in the draft Bill necessary? Are the suggested punishments appropriate?**

We take the security of our customer's data extremely seriously. We believe the new offenses proposed in the Bill are necessary and the punishments appropriate.

- **Are the proposed authorisation processes for such interception activities appropriate?**

We welcome the additional authorisation process for targeted interception and other warrants, as long as the activities of the Judicial Commissioner are not simply a rubber stamping exercise.

- **Are the definitions of content and communications data (including the distinction between 'entities' and 'events') sufficiently clear and practical for the purposes of accessing such data?**

The amending of Clause 71(9), as detailed in our previous answer, would go some way to clarifying the types of data that should be retained by a telecommunications operator and assist in understanding the distinction between content and communications data.

That said, EE still has concerns in relation to packets of data traversing our network, and specifically what is content and CD to us a network operator, and what is content and CD to a third party Over The Top (OTT) provider utilising our network. To EE, the CD is simply the information available in the header (on the outside of the packet) to allow us to route that packet from one place to another. Anything within that packet is content as we need to open the packet, irrelevant of the actual data inside. However, the definitions on the face of the Bill provide a starting point. What is required now is a detailed discussion with regards to which data types fit within which definitions and then these should be specified within the forthcoming Codes of Practice.

- **Does the draft Bill allow the appropriate organisations, and people within those organisations, access to communications data? Are there sufficient operational justifications for accessing communications data in bulk?**

EE is not in a position to comment on which public authorities should be able to access communications data or whether sufficient operational justifications have been put forward in relation to the bulk provisions under the Draft Bill. These questions will need to be addressed by Parliament as it assesses the case laid before it by the Home Secretary, based upon the recommendations from the Draft Investigatory Powers Bill Committee.

- **Is the authorisation process for accessing communications data appropriate?**

The use of Single Points of Contacts (SPOCs) is a strong, transparent, and stringent process. A SPoC must always be engaged for the acquisition of CD, is specially trained and accredited in the use of CD and will advise upon the appropriate use of all available CD. We welcome the additional safeguards in the Bill - the requirement for an independent designated person (independent from the requesting agency) to authorise all requests for CD, the

streamlining of existing legislation to ensure that all requests for CD disclosure must only be under the IPB, and the restriction on the acquisition of ICRs.

That said, the ability to sufficiently understand and query records in the internet world is very challenging as telecommunications rapidly develop and change. People live their lives online, and we have long left the traditional telephony world of a simple fixed line telephone call between two individuals. The internet makes the job of a police officer and a SPOC incredibly difficult. Industry invests time and resources in assisting Law Enforcement with the interpretation of such records, but there is undoubtedly a significant amount of work to ensure that Law Enforcement can make the best use of the data available to them. We don't want to be in position where significant time, effort and, most importantly, cost is invested in delivering complex technical capabilities that are not utilised appropriately due to lack of knowledge and awareness within the Law Enforcement community.

A point to note here is the Draft Bill sets out that a SPoC must be consulted before an authorisation is granted (60(1)) but then goes on to introduce an exception to be used in case of an emergency (60(2)). SPoC training and accreditation is essential - the current SPoC PIN system allows for verification and validation of SPoCs by telecommunications operators, ensuring data are only disclosed to authorised individuals. This is an important safeguard. EE encourages collaboration and/or partnership agreements as a means to ensure 24/7 SPoC cover, ensuring that a SPoC is always consulted and the requisite knowledge and expertise is applied to all requests for CD, except in relation to an emergency call within the emergency hour. EE expects this to be specifically addressed within the forthcoming Codes of Practice.

- **Is accessing Internet Connection Records essential for the purposes of IP resolution and identifying of persons of interest? Are there alternative mechanisms? Are the proposed safeguards on accessing Internet Connection Records data appropriate?**

An initial point to clarify is that an ICR doesn't currently exist as one whole record – it needs to be created - and some of the data needed to create an ICR is currently not retained.

The implementation of IP Address Resolution (known as IPAR) is incredibly complicated. The number of IP addresses available is not sufficient for the numbers and needs of our customers. EE therefore adopts technology which allows multiple devices (often many thousands) to utilise one public facing IP address (essentially the address which is seen by the internet). If an ownership check were to be conducted on this public facing IP address, in many cases, it would simply resolve back to the telecommunications operator who had been allocated that address, and not the specific device or devices using it. Therefore, in many circumstances on the mobile internet, the actual device being used to access internet based services is not visible. The Draft Bill attempts to address this issue by requiring certain telecommunications operators to be able to identify which devices were using which public facing IP address at specific times.

In relation to whether an ICR is essential for the purposes of IP resolution, to achieve a near one-to-one IP address to device match, for most telecommunications operators this will require the retention of destination IP address, which we anticipate may form part of and

ICR. This is because a public facing IP address may have many thousands of devices assigned to it at any one time. In order to filter down these multiple devices to a target device, it would be necessary to identify the destination IP address and the port that that device was using at a very specific time. EE does not currently have the technology to achieve this, and the massive amount of traffic passing over our network would make this a huge challenge. Further complexity and cost is introduced because of the multiple data types and limited visibility of all traffic crossing our network.

In relation to the suitability of safeguards regarding ICR access, EE believes this is a matter for Parliament, based upon operational necessity. However, we welcome the restrictive nature, laid out by the three purposes for disclosure, within the Draft Bill.

How EE retains, compiles and subsequently discloses the relevant data sets is yet to be identified. These technical complexities and the requirements to potentially retain huge amounts of additional data require more work.

- **Are the requirements placed on service providers necessary and feasible?**

Whether the requirements are necessary is a question for Parliament and the Secretary of State, based upon operational justification and proportionality. However, in terms of feasibility, it is simply not possible to answer this question definitively due to the broad scope of the Bill, and early stages of the feasibility studies associated with the new obligations.

EE has had some discussions with the Home Office on the technical understanding of an ICR, and these discussions are ongoing. This is an incredibly complex area, involving multiple transient data sets and further complicated by the proposal to utilise ICRs in order to resolve an IP address. Further discussion and consultation is required with the Home Office to understand precisely the operational requirements and how these requirements have been interpreted on the face of the Bill.

EE has also had engagement with the Home Office in relation to IPAR, and we are in a proof of concept/feasibility process. IPAR delivery is complex and will take a substantial amount of time to deliver to an operational capability - anticipated at least 18 months once requirements and technical feasibility have been completed. Until these proof of concept activities are complete and we are served with a Data Retention Notice based upon the outcome of these studies, it is not possible to provide a definitive response to the level of feasibility or costs of the proposed requirements within the Bill.

- **Should the security and intelligence services have access to powers to undertake (a) targeted and (b) bulk equipment interference? Should law enforcement also have access to such powers? Are the authorisation processes for such equipment interference activities appropriate? Are the safeguards for such activities sufficient?**

Any activities undertaken by the SIAs are a matter for that Agency and Parliament to ensure they are lawful and proportionate.

Customer trust is central to our business. The priority for us as a business is to ensure that we provide a secure and resilient network for our customers. We would not accept any activity that impacted the security of our customers data or our network.

However, we welcome the fact that before a Notice can be served upon a telecommunications operator (in order to develop a technical capability to support EI), the Secretary of State must first consult with the telecommunications operator to assess, amongst other things, proportionality, technical feasibility, cost and impact on the network and their customers. Following this process, if after a Notice has been served, a telecommunications operator still has concerns with the content of that Notice, the Notice can be referred back to the Secretary of State for review, who has a duty to consult with the Technical Advisory Board (TAB) and the Investigatory Powers Commission (IPC). This process must be enforced rigorously rather than simply a rubber stamping exercise at each stage of the process.

We believe the remit of the TAB should be expanded to cover all aspects of the legislation, including policy, strategic, technical and cost-recovery, to ensure the Board has full visibility of all relevant matters and can make informed decisions. All key stakeholders should be represented. This may necessitate renaming of the Board, to reflect its wider remit.

- **What are the advantages and disadvantages of the proposed creation of a single Judicial Commission to oversee the use of investigatory powers?**

EE welcomes the greater oversight within the Bill, brought about by the proposed introduction of the new oversight body. However, we note that the remit of the Investigatory Powers Commission does not extend to auditing the security of telecommunications operator retention infrastructure. Consistent with the general principle of a single regulator, it appears anomalous for retained data infrastructure security to fall outside of the remit of the IPC.

Additionally, we note that the IPC will have responsibility for keeping under review National Security notices, but not Technical Capability Notices. We propose that the IPC should also have oversight responsibility for Technical Capability Notices.

- **Are the new arrangements for the Investigatory Powers Tribunal including the possibility of appeal adequate or are further changes necessary?**

We welcome the extension of the jurisdiction of the IPT to include the giving or varying of data retention notices.

Additional issues

- **Cost recovery**

Although addressed earlier within our response, we believe that it is important to highlight why the cost recovery regime is essential to ensure a proportionate approach by Government. EE believes that the Bill should make it explicit that a company impacted by this legislation is able to fully recover the costs incurred. We believe that if there is no cap

on costs based upon proportionality, and the financial obligation is simply passed onto the telecommunications operator, that this could potentially result in the delivery of disproportionate solutions. A cost recovery model places a greater focus on an assessment of proportionality.

- **Authorisations/Notices**

EE supports David Anderson QC's recommendation that the distinction between authorisations and notices with respect to CD acquisition is unhelpful and should be removed. This recommendation has not been accepted by the Home Office - both authorisations and notices remain on the face of the Bill.

5 January 2016

Electronic Frontier Foundation—written evidence (IPB0119)

December 21, 2015

The Electronic Frontier Foundation (EFF) is a global nonprofit, member-supported civil liberties organisation working to protect privacy and free expression in technology, law, policy, and standards in the information society. EFF actively encourages and challenges the executive and judiciary to support privacy and safeguard individual rights as emerging technologies become more prevalent in society. With over 26,000 dues-paying members in 90 countries and over 284,000 mailing-list subscribers world-wide, EFF is a leading voice in the global and national effort to ensure that fundamental liberties are respected in the digital environment.

We have a wide range of concerns regarding the Investigatory Powers Bill, which we have laid out in our joint submission with groups including Open Tech Institute, Center for Democracy and Technology, Access Now, and the American Civil Liberties Union. For the purpose of this individual submission we will focus on the sections of the bill covering equipment interference, bulk and targeted, introduced in Part 5 and Part 6, Chapter 3.

Executive Summary

We find significant cause for concern about equipment interference, both bulk and targeted. In particular, we draw the committee's attention to the following:

- The equally wide powers provided by targeted and bulk equipment interference, and the porous nature between the two — including the undefined role, application and limits of “targeted examination warrants” (S.81(9)).

- The lack of consideration, oversight or documentation of the effect of equipment interference on parties who are unrelated to the investigation, including the powers to compel a wide range of actors as “communication service providers” under S. 101 and S.145 (4).

- That Part 5’s S.83(g) targeting of computers that are being used to test, develop, or maintain targeted interference capabilities by other actors, including private companies, may well include a range of legitimate ICT research and practice.

- The lack of consideration, oversight or documentation of steps necessary to restore equipment (especially third-party equipment) to a state prior to the act of interference in cases where the warrants expire or are cancelled.

- That the technical changes necessary to provide this information are incompatible with the ICT services duties to protect the integrity of their systems, and duty to their customers.

- We are concerned that the secret government stockpiling of vulnerabilities that the adoption of widespread equipment interference will require could undermine the

movement to a more secure and resilient digital communications infrastructure.

- We believe the compliance and actions required and legalised by Part 5 will prove at least as intrusive as the obligations for compliance enabled by national security notices, or technical capability notices as described in Part 9, with even less oversight or review.

The fundamental lack of oversight and unlimited scope of actions that can be taken or compelled by the various law enforcement and intelligence authorities under the draft's equipment interference powers must be amended and addressed in primary legislation. The current proposed statute provides so little ongoing insight into what equipment interference presently consists of, or limits on what it may become, that we believe secondary legislation or codes of practice will be unable to pierce the secrecy and ambiguity embedded in the bill's current framework.

We strongly urge the committee to push for equipment interference to be separated into separate legislation that can be more carefully considered. Without better safeguards, "future-proofing" these powers will simply future-proof equipment interference from Parliamentary and even executive oversight, while undermining public confidence in digital communications and the integrity of the global communications infrastructure, and their own property and possessions.

Statement of concern

1. **Equipment Interference: Hacking by Any Other Name**

2. The new equipment interference provisions describe a broad range of potential actions by law enforcement and the intelligence agencies. While the Secretary of State's explanatory document describes the potential use of this power as "encompassing a wide range of activity from remote access to computers to downloading covertly the contents of a mobile phone during a search", this barely scratches the surface of what equipment interference may be capable of.

3. The common term for "equipment interference" is "hacking": breaking into and remotely controlling devices. It permits third parties to transform a general-purpose device such as a modern smartphone, laptop, or desktop computer into a surveillance machine.

4. Equipment interference is an extremely intrusive power, especially in the hands of governments and law enforcement agencies, whose activities are frequently shrouded in secrecy from the oversight of civil society and are only weakly checked by judicial or legislative powers. Equipment interference can give an attacker complete control of a communications device, successfully circumventing all encryption, granting access to all data and metadata on the device including, but not limited to, passwords for other systems, location data, cameras, and microphones), and allowing the attacker to execute arbitrary malicious code. It can be abused to plant incriminating evidence, deploy permanent malware, or rewrite existing data to

any end.

5. Because it is so intrusive, equipment interference carries with it a tremendous possibility for abuse, and requires the strictest safeguards and oversight.

6. Bulk and Bulkier Equipment Interference

7. The current bill subdivides equipment interference into "targeted" and "bulk" interference. This is a potentially misleading description of the division created by the bill. A look at the set of potential subject-matter for targeted warrants in S.83 demonstrates that they may be applied to wide set of equipment and circumstances, including "equipment that is being, or may be being used, for the purposes of a particular activity or activities of a particular description". Targeted equipment interference is not targeted to a person; equipment affected by "targeted" interference may also be used by many other, innocent users.

8. Bulk interference contains none of the subject-matter restrictions of S.83; instead, bulk equipment interference facilitates the obtaining of overseas-related communications, private information, and equipment data (S.135 (2)). However, the broad range of intrusive actions that might be taken under both targeted and bulk interference remains the same. Only the grounds of the warrant are different.

9. Grounds, Conduct and Steps: The Invisible Damage of Equipment Interference Warrants

10. This brings us to one of the problems with the oversight and authorisation system built into the current bill. The Secretary of State, Scottish Ministers, law enforcement chiefs, and Judicial Commissioner are involved in determining whether the warrant is *necessary* on the grounds defined as appropriate by the bill, and that the conduct authorised by the warrant is *proportionate* to what is sought to be achieved (see Ss.84,86,87, and 89).

11. This decision is based on the contents of the warrant. This contents for targeted warrants is described in S.93 (4) as "(a) the type of equipment that is to be interfered with, and (b) the conduct that the person to whom the warrant is addressed is authorised to take."

12. However, the powers in targeted equipment interference warrants extend much further than just the conduct of the warrant-holder. As S.81(5)(b) notes, it also authorises conduct by any other person, and includes, via S.101, a power to require compliance from communications service providers (CSPs). The recipients of bulk interference warrants have similar powers under S.135(4) and S.145(4). What process ensures that the conduct of these other entities (not warrant-holders) is necessary and proportionate? How would accountability be established and routinized as a matter of democratic practice?

13. ***One of the greater risks to the public interest and the integrity of digital***

***communications arises from these third-party requirements*.** This is because equipment interference can include such a wide range of possible actions, including the re-engineering of software to undermine its own privacy protections, and transform it into surveillance systems. The ultimate actions taken by the authorities and CSPs are not required to be described within the warrant, and the safeguards of the bill are silent on limits to these actions, or requirements to limit potential side-effects on CSPs, their other customers, or the international communications infrastructure as a whole.

14. The bill's safeguards concern themselves with the *grounds* of the warrant, and a vague description of *conduct*. But it is the individual technical *steps* required from CSPs and third-parties that may well pose the most risk of overreach.

15. **Section 101 Compliance, A New Burden on Technology Companies and Technologists**

16. Previous law (Intelligence Services Act 1994, S.5 and the Police Act 1997, Part III) authorised action by intelligence agencies and law enforcement, but did not compel private parties to assist. S.101 and S.145(4) of the proposed new bill confer for the first time an explicit duty on telecommunication providers to assist with the implementation of an equipment interference order.

17. This requirement widens the capabilities of law enforcement and the intelligence agencies from their own skillset and personnel, to include that of any and all organisations whose resources they might commandeer to execute an order. This represents a significant new responsibility for technology companies and technologists within the reach of British law.

18. The proposed bill's definition of who might be included in such compelled actions is unreasonably broad. 101(5) defines "relevant telecommunication provider" as anyone who provides a telecommunication service, or could effectively control a UK telecommunication service (or a service that could be controlled from the UK). The word "relevant" in the bill therefore carries little practical meaning.

19. The limits on what these persons and organisations might be required to do is also left largely undefined. According to 101(2), the steps taken by CSPs required by warrants served by law enforcement need to be pre-approved by the Secretary of State, and be determined to be necessary and proportionate by him or her. But no such determination is required in the case of targeted equipment interference warrants presented by intelligence agencies. Under these warrants, telecommunication providers must obey any instructions given by or on behalf of the person to whom the warrant is addressed: but these steps are not described or included in a S.84,86 or S.87 warrant. (See the different documentation requirements described in S.101(1) and S.101(2), and the limited scope of S.101(4)).

20. The only qualification to this broad order is 101(6), which states that it "is not

required by virtue of this section to take any steps that it is not reasonably practicable [for them]", but with no guidance as how "reasonably practicable" may be determined, how providers might resolve disputes about practicability, or how users will be able to hold anyone accountable for rights-violations associated with such steps.

21. Telecommunications providers are further bound by the Section 102 gag order, which may prevent them from conferring with other experts in the field, other telecommunications providers that may have received similar order (and possibly even counsel) before executing the orders given by the warrant holder.

22. Note also that "relevant telecommunications provider" may include an engineer or other employee who has control of a telecommunications system. Control is generally interpreted in contexts similar to this as *legal* control, but equipment interference by intelligence agencies has historically involved taking control of systems without legal right to do so[2].

23. It may be then that a person with control of a telecommunications system may be interpreted here as an individual who has the *capability* to interfere with a telecommunications system, but not legal control. That is to say, a warrant might be served on British Telecom, for example, to compel them to interfere with a device they neither own nor legally control, such as a phone using their network in order to access its voicemail.

24. Similarly, an order might be served not on British Telecom as the provider of the telecommunication service, say, but upon an individual network administrator within British Telecom who has *effective* control of its systems, if not the legal right or management permission to use it for the purposes required by the warrant.

25. Such a power to incentivize an individual to secretly act against his employer's interests is novel in traditional law, but is already common practice within the intelligence community. GCHQ has a section called Humint, "responsible for identifying, recruiting and running covert agents in the global telecommunications industry"[3]. Given existing practice, it is vital to clarify whether such behaviour are intended to be sanctioned within the Investigatory Powers Bill's framework.

26. To summarise: under the new proposals, GCHQ can compel a wider range of technology companies within reach of UK law (and potentially individuals within those companies) to do anything within their power to transform the hardware or software they control into a surveillance device. They are not allowed to tell anyone what they have done to that technology, and will face criminal penalties if they do so.

A Government Power to Deploy Malware, Regardless of Consequence

27. "Equipment interference" carries with it the implication that the power is restricted

to impeding normal equipment operations, but may also include adding unexpected new functionality to a device.

28. A company, or an individual within a company, for instance, might be compelled to insert malicious code into an existing product for the purposes of targeting equipment "of more than one person or organisation, where the interference is for the purpose of the same investigation of operation" (83(c)), in order to obtain any communications or private information.

29. This code could be placed into any piece of software or hardware accessible by the company or individual. The only constraint is that it must be "reasonably practicable" (101(6)).

30. The limit placed on both bulk and targeted equipment interference—that such acts do not violate S.2(1) (as in S.81(6) and S.135(5))—is no effective restraint, because the data collected would not necessarily be transmitted over a telecommunications network. Indeed, the most intrusive forms of data collection, including the use of laptops, smartphones and other electronic equipment to spy on its users, would not be excluded by this provision—especially when stored communications are expressly permitted to be collected, as they are in S.81(6) and S.135(5).

31. To give one example of how equipment interference, mediated by a telecommunications provider, might operate: In 2009, a software update was sent to all owners of Blackberry devices using the Etilsat network in the United Arab Emirates. The software required manual agreement by the end-user. If accepted, the new software transformed their mobile phone into a spying device, which, as the manufacturer of Blackberry, Research In Motion (RIM), wrote, "enabl[ed] unauthorised access to private or confidential information stored on the user's smartphone."

32. RIM warned its own users about this software, because the update masqueraded as a legitimate upgrade to improve performance of the devices. RIM also had a strong incentive to protect its hardware's reputation as a high-security device, as Blackberry smartphones had been sold to multiple government and international financial institutions. If RIM had been discovered to be the real author of such an update, it would have destroyed its reputation as a guardian of its customers' data.

33. Under the proposed law, a British company could be compelled to distribute a similar update in order to facilitate the execution of an equipment interference warrant, and ordered to refrain from notifying their customers as RIM did. Such an update could be targeted at an individual, an organisation, or many organisations related to a single investigation.

34. Such updates are eminently "practicable" for companies to deploy, as they already maintain the infrastructure to provide such updates. For proprietary commercial software, it is also theoretically possible to comply with a secrecy requirement regarding the content of these updates.

35. However, because this software runs on end-user systems, there will always be a chance that such a targeted "back door" to private data would be revealed. While a company may be compelled to keep silent regarding the purpose of an update, other external experts can examine the contents of the updates and reverse-engineer their purpose[4].

36. Such a revelation would effectively destroy a telecommunication provider's reputation for protecting its end-users and the integrity of its systems: however, the request would be "reasonably practicable", if practicable is defined merely as something that a company or individual can practically achieve.

37. Note too that a broad distribution of such spyware might be more "reasonably practicable" than a targeted distribution. It may often be easier and more covert for a company with an existing software update infrastructure to roll out an update for every user, than it would be to distribute an update to a single user or set of users.

38. **Destroying Trust Across the Public and Private Sector**

39. Because "relevant" appears to have no real power as a limiter in the bill, the law could also be used to involve organisations and individual technologists who might not be expected to be involved in espionage or assisting law-enforcement. "Telecommunication providers" also covers a broader segment of the communications industry than might be expected by an everyday understanding of the term.

40. In particular, the expansion of the definition of "telecommunications service" in 193 (12) (first introduced in the Data Retention and Investigatory Powers Act), means that individual Internet services such as Facebook, Twitter, Dropbox, Microsoft Office Online, content delivery networks such as Akamai, Fastly and CloudFlare and others are included in the definition. Government departments such as the National Health Service or academic networks could also be included.

41. This means that, under the equipment interference provisions, a large part of the Internet industry, both private and public sector, could be required to act as a delivery mechanism for malware. Under the proposed law, GCHQ could compel any Internet company providing a service to configure their web servers to serve surveillance malware to the devices of those visiting to their website. Email providers could be compelled to append surveillance software as attachments to legitimate email.

42. Again, this use of Internet websites to deliver malware is a common practice of criminals and malicious state actors. Yahoo's online advertising network has been used to insert malicious software[5] and attackers connected to the Chinese state broke into Amnesty Hong Kong's website to deliver surveillance software to its visitors,[6] to give just a few examples.

43. No constraints exist in the proposed law to limit what systems might be used for such malware delivery purposes. Indeed, under the duties regarding intelligence orders made under 101(1) (as opposed to 101(2) which requires steps to be approved by the Secretary of State), even the Secretary of State or Judicial Commissioners will not be informed of precise steps taken by telecommunications providers. It is therefore difficult to understand how either ex ante or ex post oversight and accountability can be implemented.

44. **A Note on State-Deployed Malware**

45. Whether or not equipment interference will require the enforced co-operation of third parties, it will often require the exploitation of security flaws in the targeted equipment. For instance, if malware is distributed by email or via the web, it will first need to defeat the anti-malware protections of an anti-virus program, the web browser or email client, and finally the security defenses of the underlying operating system.

46. States are already known to bid for security flaws (or "vulnerabilities") on the open market, competing with vendors and others to obtain confidential information on recently discovered problems with software.

47. For government to successfully use these vulnerabilities, they must keep them secret from companies responsible for securing communications systems, to prevent them from fixing the underlying insecure system before they can be used. (Vulnerabilities that are not yet known or fixed by the responsible vendors are called "0-day" vulnerabilities.)

48. This places governments practicing equipment interference in direct opposition to the overall security and integrity of the global communications infrastructure. To maintain an equipment interference capability, governments will need to prevent vendors and researchers from fixing dangerous security flaws.

49. If the UK government insists that equipment interference, including the deployment of malware and the undermining of vendor and user security, is a legitimate function of the state, the bill should also include provisions to ensure transparency and oversight over the collection of 0-days and similar tools, and oversight to limit this practice's effect on the overall security and integrity of communications infrastructure.

50. **Bulk and Targeted Equipment Interference Will Require Much Stronger and Equivalent Restrictions and Oversight**

51. All of the above examples apply equally to bulk and targeted equipment interference, demonstrating that the division of these two powers in the bill is

unrelated to the level of oversight and clearly-defined limits that both powers require.

52. Even the pre-existing division between bulk and targeted equipment interference is not as compartmentalised as the bill would imply. Part 5 speaks of a "targeted examination warrant" that would provide for access to material obtained under a bulk equipment interference warrant (see S.81(9)). No description, safeguards or limits are described for this warrant. Either the existence of targeted examination warrants under Part 5 is a drafting error and should be removed, or much stronger controls placed on the examination of material gathered under a bulk equipment interference beyond its original grounds.

53. **The Unacceptably Broad Reach of Section 83(g)**

54. A targeted equipment interference warrant may relate to 83(g) "equipment that is being, or may be used, to test, maintain or develop capabilities relating to interference with equipment for the purpose of obtaining communications, private information or equipment data." This is alarmingly broad language, since capabilities relating to interference with equipment for the purpose of obtaining communications etc. includes private companies that build such software for use by governments and law enforcement (such as Boeing or Raytheon), private companies that build deep packet inspection tools for managing networks (such as Cisco Systems or Blue Coat), private security researchers using the tools of the trade to reverse engineer communications systems in order to find vulnerabilities, and academic researchers who do the same (such as Carnegie Mellon University researchers who recently attracted attention with their research about how to de-anonymize users on the Tor network).

55. Potentially, this section could cover anything from a laptop running standard network debugging tools to source code repositories such as GitHub, provided that they meet the other requirements for a warrant. This section may be intended to allow GCHQ to disable equipment interference that may be targeted at UK persons, but as written it puts significant academic and security research at risk.

56. **Clearing Up the Mess: Amelioration, Remuneration and Notification**

57. Both targeted and bulk equipment interference provisions envisage the end or termination of an equipment interference warrant. Warrants can expire (Ss.94-95 and S.141-142), be cancelled (S.98 and S.144) or be retroactively refused by the Judicial Commissioners (S.92).

58. The assumption within these procedures is that ending a warrant restores the equipment to its previous, uninterfered-with, state. The parallel made is with a surveillance warrant, where once the surveillance is concluded, no additional steps need to be taken.

59. This is not true with equipment interference. At the very least, bill should make clear that malware installed or distributed under the warrant must be removed, services and equipment interference restored to their initial conditions, and CSPs required (and possibly remunerated) to restore the privacy and security of their services. The process for terminated warrants should include statutorily required post-hoc reviews.

60. Notification should also be considered as an integral part of restoring the status quo after a warrant has expired or revoked, particularly if it did so as a result of a Judicial Commissioner rejection of an emergency warrant.

61. In general, the Investigatory Powers Bill is silent on notification, either to innocent parties, or third parties commandeered to interfere with their own or others' equipment. The committee should include obligatory notification requirements, as a vital tool of transparency and to prevent overreach.

62. **Limitations on Realtime Wiretaps**

63. S. 81(2) appears to indicate that an equipment interference warrant can be used to obtain a very broad range of data (ie “communications”). S. 81(6) attempts to exclude the interception of communications that are not “stored communications” (ie realtime wiretaps). However, these intentions appear to be thwarted by language that only places these limits communications obtained under S. 81(3) and not S. 81(2).

64. **The James Bond Clause**

65. S. 81(5) and S.106(5) states that a targeted equipment interference warrant authorizes “any conduct that is necessary to do what is expressly authorized in the warrant.” Subsequent language only goes on to add to the list of conduct that is allowed, rather than providing any sort of narrowness or specificity. This section fails to specify who is empowered to decide what constitutes “necessary” conduct. Furthermore, there is no indication of whether “necessary conduct” must fall within the bounds of the law,or if this section is meant to grant immunity from prosecution for conduct carried out in the process of carrying out the warrant. It also makes no mention of the interaction between UK law, and the law of country where such conduct may take place. As currently written, S. 81(5) could be interpreted as granting the sort of powers normally associated with the fictional world of James Bond's intelligence services, rather than conduct within the rule of law.

66. **Conclusions f**

67. The broad scope of machine interference warrants, the range of affected providers who may be compelled to assist, and the large set of potential targets, make this power one of most potentially intrusive in the new bill. It however lacks many of the

review and oversight mechanisms attached to other powers.

68. Without sufficient oversightthese powers would undermine trust in a broad range of online services, technology companies, academic research, and government services. Without clarity of the limits of such powers, global companies would choose to move their services out of the reach of UK individuals and organisations.

69. The bill's division between bulk and targeted equipment interference is unclear and porous. Both powers create substantially new capabilities to interfere and damage with communications services and affect innocent users. Both should require equally high levels of oversight and review.

70. This review must extend to the steps taken by CSPs and others to implement the warrant. Such actions must be anticipated and documented in the warrant, and reviewed by an independent technical and civil liberties body.

71. The current language of the bill means that such oversight is impossible. This will not be amendable with secondary legislation or codes of practice, since the most dangerous elements of the power are currently hidden from review by Parliament, the judiciary, and in some cases, even the Government itself.

72. Equipment interference is a deeply intrusive power, with no history of successful oversight or control. Rather than abandoning specific language in the pursuit of making this power “future-proof”, Parliament should carefully consider whether such a power can ever be proportionate.

73. We urge the committee to consider separating it from the rest of the legislation for closer consideration, under a more reasonable time-frame. .

Outstanding questions

Q1: What is the practical meaning of “relevant” in the bill’s definition of “relevant telecommunication providers” 101(5)?

Q2. Does it mean that the person must have the targeted equipment under its legal control, or only its effective control? Can providers be compelled under law to interfere with equipment that they do not themselves own or legally control?

Q3: Can individuals be compelled to assist in complying with the warrant to interfere with equipment that they do not themselves own or legally control?

Q4: What oversight to provide for necessity and proportionality, and consistent process and requests are available for steps taken under warrants granted under section 84, 86 and 87, if the checks in 101(2) and 101(4) do not apply?

Q5: Can the descriptions of all warrants be expanded to include documentation of the

conduct required of third-parties, including CSPs?

Q6: Can the consideration of "necessary" and "proportionate" be similarly expanded to include the steps taken by CSPs and all other third-parties?

Q7: What are the criteria for what is "reasonably practicable" in 101(6)? Is it based on current capabilities, financial burden, or consequences for the provider if the co-operation is revealed?

Q8: How far does the 102 gag order extend? Are providers allowed to discuss the actions they are required to take with counsel? With external technical experts? With internal staff?

Q9: What practical limits (with examples) do S.81(6) and S.135(5) place on equipment interference warrants?

Q10: What are the practical differences between the powers to order telecommunication providers to comply with warrants under Part 5, and the compelled actions under national security notices, and technical capability notices operating under National Security Notices (S.188-)?

Q11: What process for challenging and redress will telecommunication providers have for demands that are unreasonable or impracticable?

Q11b: Is this process available only post facto?

Q12: Given that refusing to comply with an order on the basis of its practicality may be seen as "prejudicial to … national security, the prevention or detection of serious crime, or the economic well-being of the United Kingdom", or "jeopardise the success of an intelligence or security operation or law enforcement operation" 169(5), or "duly impede the operational effectiveness of an intelligence service, a police force, a government department or Her Majesty's forces" 169(6), can the Judicial Commissioners ever refuse to authorise or revoke a warrant on the basis of its impracticality, or the lack of necessity or proportionality of the conduct it requires or acts it compels?

Q13: If a demand is successfully challenged as impracticable, what requirements are in place on the Secretary of State or owners of a warrant to note this in future orders to other telecommunication providers?

Q14: Will the imposition of an order that previously determined as impracticable, onto another telecommunication provider (who chooses not to challenge the order) be deemed as an error under S.171? Or will the acceptance of a particular order by a single telecommunication provider establish a practice as reasonable and practicable for all similar telecommunication providers?

Q15: Does GCHQ have any guidelines for deciding whether to stockpile a 0-day vulnerability that they may use to facilitate future equipment interference?

Q16: Will GCHQ report on its stockpile of 0-days in the same manner as the NSA has done?

Q17: What kind of data is section 83(g) meant to obtain that connect be obtained under other authorities granted in this bill?

Q18: What provisions will be made to restore interfered equipment to its initial state?

Q19: Who will be notified in the event of the expiring, cancellation or invalidating of an equipment interference warrant?

Q20: What kinds of targets are appropriate for equipment interference under S. 83(g)? Security researchers? Anti-virus companies? Academic institutions?

Q21: Are there any limits to what could comprise a "relevant system" in S. 82? Can you give some examples?

Q22: Are there any limits to what constitutes "necessary action" in S 81(5)? Does action have to be within the limits of the law? If not, does this language grant immunity from prosecution?

21 December 2015

Entanet International Limited—written evidence (IPB0022)

Background

1. This submission is made on behalf of Entanet International Limited, a wholesale communications and Internet Service Provider serving UK businesses through channel partners. The author, Entanet's Product Manager, is a non-practising solicitor who gave evidence to the Joint Parliamentary Committee on the draft Communications Data Bill in 2012.

Timescale

2. We invite the Committee to consider whether three weeks is sufficient time to take evidence, given that when the above Bill was scrutinised the Joint Parliamentary Committee concluded that there "should be a new round of consultation with technical experts, industry, law enforcement bodies, public authorities and civil liberties groups".
3. Entanet were not consulted on the Draft Investigatory Powers Bill. Our trade body, the Internet Service Providers Association, received an invitation from the Home Office to attend an informal briefing on 24th November; the day after your committee convened.

Responses to Questions

- *Has the case been made, both for the new powers and for the restated and clarified existing powers?*

4. Paul Lincoln, Home Office Director of National Security, in his evidence said current spend is around £90m and they would expect this to double with the new Bill, hence the £174m which has been set out to cover 'reasonable' costs Communication Service Providers will incur due to the Bill.
5. We believe taxpayers should know how their money is being spent: the current position is opaque, and the justification for more money non-existent on the basis of this answer. Is it the case that this Bill is significantly cheaper than previous efforts because some of the mass surveillance costs were covered under the recent Anti-Terrorism legislation instead?
6. As an Internet Service Provider, we have not been consulted and could not provide an estimate of cost. We are concerned that the provisions in the Draft Bill about confidentiality surrounding notices would hamper any attempt to negotiate with suppliers if we were required to obtain an estimate.
7. If, as Richard Alcock, Programme Director of the Communication Capabilities Directorate at the Home Office, has said in evidence, the Home Office to date has always covered 100% of CSP's costs, can this not be made a term of the bill, rather than the will pay "greater than zero" wording currently used?

- *Are the powers sought legal?*

8. We invite the committee to consider what legal advice would be given to an Internet Service Provider served with a subject access request under the Data Protection Act for retained Internet Connection Record data, given the secrecy obligations relating to notices under the draft Bill. Which provision wins?

- *Are the powers sought workable and carefully defined?*

9. Who do the new powers apply to? The definition of Communications Service Provider is extraordinarily wide – it could extend to a coffee shop offering free Wi-Fi. We note that in the first oral evidence session Home Office witnesses refused to elaborate as to what exactly a CSP could be, but did say notices may be served on some software providers.

- *Are the technological definitions accurate and meaningful (e.g. content vs communications data, internet connection records etc.)? Does the draft Bill adequately explain the types of activity that could be undertaken under these powers? Is the wording of the powers sustainable in the light of rapidly evolving technologies and user behaviours? Overall is the Bill future-proofed as it stands?*

10. Internet Connection Records are a new concept, and on the face of the Bill it is not clear to us what they are. We believe this ambiguity is deliberate, to allow scope creep. The cost on Communication Service Providers is significant, inasmuch as these records do not currently exist, unlike telephony Call Data Records.
11. At an informal briefing by the Home Office we were told they are not a technical construct but a "combination of bits and pieces of data" including:

- destination IP
- URL or rather part of it; the full string is content, the part to the left is communications data
- Date and time
- Who the person was; an identifier

12. The ISPs present pointed out (a) IP addresses don't correspond to individuals and never will (b) ISPs deal in packets, unless they choose to run mail and DNS servers. The data the Home Office appear to want doesn't necessarily exist in the form described, and if this is what is wanted, should it not be set out in the draft Bill? Any argument that ICRs are akin to telephone records is flawed: what can be inferred about a person's personal life from websites visited (an ever-increasing part of everyday life) is far more intrusive than phone records (a decreasing mode of communication and less explicit about intent).
13. Richard Alcock, Home Office Director of the Communications Capability Development Programme, said in evidence that the Home Office had a good relationship with Communication Service Providers and that they had had many meetings with providers that were likely to be served with retention notices. We suggest that it should be clear on the face of legislation what is being done, and that the scope of the draft Bill should not be whatever is decided in secret.
14. For there to be an informed debate in the House, it should be clear on the face of the Bill what intrusion there is into citizens' privacy.

15. The request filter is also a new construct. In evidence Richard Alcock said the Home Office only viewed the request filter as a safeguard which filters out irrelevant information data. In order to do this it must contain irrelevant information data and there is therefore a risk that, being we understand a large database containing by definition information on innocent citizens, it could be abused by those with access to it, for example, to track an ex-partner. The complex queries such a database allows make the extent of intrusion difficult to quantify or oversee on the face of the bill.
16. Does the filter already exist? We presume there must at least be a specification for it for a costs estimate to be arrived at. Ought this not to be shared with the House?
17. It is all very well for Paul Lincoln, Home Office Director of National Security, to say that their systems are "built to stringent standards" – no doubt TalkTalk thought the same, before their systems were attacked recently. We submit that it is magical thinking to imagine a computer system can be built that cannot be compromised.
18. Does the Bill allow a notice forcing a provider to break encryption? We are not clear on this point. If the Bill is to stand, it should at least include on its face a provision that third parties be required only to do what is "technically feasible".

- *Are the powers sought sufficiently supervised?*

19. Part 7 of the Bill includes extremely wide powers for the collection of bulk personal data sets. We recommend that this is reviewed and limited, as these data sets by definition will include information on innocent citizens.

- *To what extent is it necessary for (a) the security and intelligence services and (b) law enforcement to have access to investigatory powers such as those contained in the Draft Investigatory Powers Bill?*

20. As former MP Dr Julian Huppert points out in his evidence, in a climate of "evidence informed approaches to policy making" it is regrettable that there is so little evidence provided by the Home Office to justify the legislation, particularly in terms of cost and benefit, given the experiences of, for example, Denmark who have tried and retired similar measures as there was no benefit found.

16 December 2015

Equality and Human Rights Commission—written evidence (IPB0136)

Introduction

Three recent expert reports[303] made numerous recommendations to reform the present investigatory powers regime. Those reports examined a changed surveillance landscape after Edward Snowden revealed the scale of the UK intelligence and security agencies' electronic surveillance capabilities through the TEMPORA programme and through access to large volumes of electronic data under the PRISM and other surveillance programmes of their US counterparts.

Litigation brought against the UK intelligence and security agencies as a result of those revelations challenged the lawfulness of the present legal framework. Many of these cases are awaiting determination[304]. As a result of the revelations and subsequent cases, the UK Government has acknowledged the existence and use of certain surveillance powers.

The draft Bill seeks to replace and streamline the current legislative framework, most notably the Regulation of Investigatory Powers Act 2000 (RIPA). The EHRC has said since 2011[305] that RIPA is outdated and urgently in need of replacement.

The challenge is to ensure the intelligence, security and law enforcement agencies have the required capabilities necessary in a rapidly changing digital age to protect the public from terrorist threats and to prevent/detect crime, while ensuring those powers are subject to necessary constraints and safeguards to ensure they are only exercised in accordance with the law and only at the expense of qualified individual civil liberties (ie. those that can lawfully be restricted) in circumstances where demonstrably necessary and proportionate.

Overview

Our assessment of the human rights implications of the proposals in the draft Bill is provisional at this stage because we do not have sight of the full legal framework. This includes Codes of Practice and operational guidance which will contain practical explanation of how to exercise the powers in the draft Bill in compliance with human rights requirements. We recommend Codes of Practice in particular are published

[303] The Intelligence and Security Committee of Parliament, Privacy and Security: A Modern and Transparent Legal Framework, March 2015; A Question of Trust: Report of the Investigatory Powers Review June 2015; A Democratic Licence to Operate, Royal United Services Institute 15 July 2015. The Commission gave evidence orally and in writing to the ISC's inquiry and made detailed written submissions to the review led by David Anderson QC. http://www.equalityhumanrights.com/legal-and-policy/our-legal-work/consultation-responses/investigatory-powers-review-call-evidence.

[304] Big Brother Watch and Others v United Kingdom (application number: 58170/13 and 10 Human Rights Organisations v the UK (App No. 24960/15). R (Davis) v Secretary of State for the Home Department 2015 EWHC 2092 (Admin), in which the Court of Appeal has recently referred the question of DRIPA section 1 (bulk communications data collection requirement) compatibility with the EU Charter of Fundamental Rights to the CJEU, seeking clarification on its approach in the Digital Rights Ireland case

[305] See EHRC research report: Protecting Information Privacy, 2011

alongside the Bill to improve understanding and enable scrutiny of the full legal framework proposed. Furthermore, case law is still evolving concerning UK State surveillance powers and human rights: a number of cases remain outstanding, the outcome of which may have a significant bearing on the shape of the legislation.

The Home Office memorandum on the Investigatory Powers Bill and the European Convention on Human Rights (Home Office ECHR memorandum)[306] accompanying the draft Bill identifies the European Convention rights that are engaged in this context. It refers to Articles: 2 (right to life), 8 (respect for private and family life), 10 (freedom of expression), 14 (non-discrimination in the enjoyment of Convention rights) and Article 1 of Protocol 1 (the right to property) as well as relevant jurisprudence.

The purposes for which each of the powers contained in the draft Bill can be exercised accord with human rights requirements: protecting national security, the economic well-being of the country and preventing or detecting crime. These are legitimate aims for the purpose of interfering with qualified human rights such as the rights to privacy and free expression.

The draft Bill proposals aim to place investigatory capabilities and powers under an updated legal framework, which improves the prospect of those powers being 'in accordance with law' for the purposes of human rights law. This requires the powers to be precisely formulated in clear, accessible and foreseeable rules and circumscribed to prevent arbitrary use and abuse.

In addition to the legal guarantees which are set out in the legislation concerning the scope, grounds and duration for using these powers, the 'double-lock' prior warrant authorisation process that applies to most powers in the draft Bill aims to ensure that the powers are used in compliance with the law and human rights standards such as necessity and proportionality.

After the event oversight is to be streamlined in the form of a new Investigatory Powers Commissioner (IPC) responsible for inspection, audit and public reporting on the use of all the powers. That is in addition to an individual right to seek redress from the Investigatory Powers Tribunal (with a new domestic right of appeal against that tribunal's judgments on points of law), which can order disclosure of serious errors to affected individuals where it is in the public interest. A new criminal offence is to be created concerning unauthorised access to data. The parliamentary oversight role of the security and intelligence services through the Intelligence and Security Committee is preserved, as is the data protection inspection and regulation regime through the Information Commissioner's Office (ICO).

Our provisional analysis is that in many respects the draft Bill proposals considerably improve the legal framework governing investigatory powers in the UK and make

[306] Investigatory Powers Bill European Convention on Human Rights Memorandum https://www.gov.uk/government/publications/draft-investigatory-powers-bill-overarching-documents.

important progress towards meeting relevant human rights requirements.

Proposals to further improve the draft Bill

Underpinning complex legislation with clearly articulated principles

In our 2011 research report[307] we recommended new legislation should contain a set of agreed principles that help to understand, apply and interpret the legislation, helping to ensure it is fit for purpose and stands the test of time. Those principles should include reference to compliance with human rights law and we recommend as a starting point those principles and key tests articulated in the respective reports of David Anderson QC and the Royal United Services Institute.

Judicial review under the 'double-lock' warrant process

A 'double-lock' mechanism applies to the exercise of most powers and requires initial approval of the warrant to be reviewed by a judicial commissioner.

We recommend that the standard of review by judicial commissioners should be clearly explained in a Code of Practice to make clear the requirement that judicial commissioners must apply the same principles as would be applied by a court on an application for judicial review should include intense scrutiny to whether the measure is necessary and proportionate.

Collection and acquisition of communications data

Communications data are defined as information about a communication other than the actual communication content. Such information includes information about the sender and the recipient (for example phone numbers and address) as well as information such as the fact, location and time of a communication. It also includes internet connection records.

Part 4 of the Bill provides a power for the Secretary of State to require the retention of communications data by a communications services provider for up to 12 months. This may include retention of internet connection records, which are records of internet services that have been accessed by a device. They may include a web address along with time and date of access and a service name (e.g. www.facebook.com) but not a full web address as this would be defined as content. It would show that a person has used, for example, Google but not what searches have been made on the site.

Approximately 45 public bodies will have the power to access communications data for a variety of purposes. For most, the authorisation process comprises securing approval to access communications data from a designated person or single point of contact within the organisation but separate from the investigation or operation. That is a much lower level of authorisation than the 'double-lock' process.

[307] Protecting Information Privacy, 2011

In our view the proposal could be substantially improved by placing the power to grant authorisations for access to communications data in all cases in the hands of an independent administrative body. We recognise the relatively high number of such authorisations may make it impracticable for the same level of scrutiny by judicial commissioners as is envisaged for certain other powers. We suggest instead that consideration be given to having a separate system of independent administrative authorisation, perhaps by officers at the IPC, who could refer novel and contentious matters to the judicial commissioners.

Bulk powers concerning interception, acquisition of communication data and equipment interference

These powers appear to permit wide ranging bulk interception, acquisition and equipment interference including of communications and equipment in the UK in pursuit of relatively generalised operational purposes, and their selection for examination in many instances by reference to individuals known to be in the UK.

We consider further attention should be given to safeguards that clearly limit the basis on which bulk material can be examined and that will ensure safe retention and destruction of material. Such safeguards might include more narrowly defined purposes.

We have previously submitted to the ISC inquiry that bulk surveillance powers aimed at communications abroad are likely to disproportionately affect members of some ethnic minority communities in the UK and may therefore, subject to justification, be indirectly discriminatory. This remains a concern in relation to the draft Bill. We recommend the potentially discriminatory impact of these powers should be considered as part of the scrutiny of the draft Bill.

The power to retain information

Information only has to be destroyed, for example, when there are “no longer any relevant grounds for retaining it” (clause 40(5)), meaning “retention is not necessary or not likely to become necessary” (clause 40(6)).

This means it can be retained even where there is no current utility if it is considered it may be of future utility

In Digital Rights Ireland, in the context of retention of communications data, the Court of Justice of the European Union (CJEU) criticised the failure in Directive 2006/24/EC (the Data Retention Directive) to make any distinction in retention periods between categories of data on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned.

In the context of retention of DNA profiles of individuals who have not been convicted of an offence, the court has held a blanket or indiscriminate approach to retention of such

information to be unlawful in breach of Article 8 ECHR.[308]

We would anticipate that a Code of Practice will set out appropriate safeguards for data retention, such as an express requirement to review, an automatic destruction period subject to exceptional circumstances, and different periods for different types of information. If so, it would be very helpful if a draft Code of Practice containing such safeguards were published alongside the Bill to aid scrutiny of these provisions. In light of developing case law we anticipate that such measures are likely to be required to ensure that the regime for retention of information is human rights compliant.

National Security Notices

Under clause 188, the Secretary of State may give any UK telecommunications operator a notice ("a national security notice") requiring them to take such steps as the Secretary of State considers necessary in the interests of national security provided that the Secretary of State considers that the specified conduct is proportionate to what is sought to be achieved. The notice cannot include steps for purposes which require a warrant or authorisation.

In order to provide additional safeguards over the exercise of this power, and promote public confidence in its use, we consider this power should be subject to judicial approval and automatic referral to the IPC for review of how and why the power is being used.

Consistent safeguards for confidential information held by certain professions

There are additional safeguards in the Bill for MPs, and in some parts for journalists, but not for lawyers and other professionals who hold confidential material such as doctors.

The Home Office ECHR memorandum states that a Code of Practice will set out that particular consideration must be given where the subject of the interception may reasonably assume a high degree of privacy or where confidential information is involved. This will include confidential journalistic material and legally privileged material.

- The memorandum states that where an application for a warrant is likely to lead to privileged material being intercepted, it will need to set out an assessment of the likelihood of that interception and the steps that will be taken to mitigate the risk. Where it is intended that privileged material be intercepted, the warrant will only be granted where the Secretary of State is satisfied that there are exceptional and compelling circumstances that make it necessary. Additional safeguards regarding the handling, retention and disclosure of the privileged material will apply. These additional safeguards are welcomed.

Where the intention is to acquire journalistic material, the memorandum states the application for the warrant should set out the reasons why and why it is considered necessary and proportionate to do so.

In the context of journalistic information, not only is compliance with the right to privacy

[308] S and Marper v United Kingdom in the European Court of Human Rights (2009) 48 E.H.R.R. 50.

protected by Article 8 ECHR required but also with the right to freedom of expression protected by Article 10 ECHR. Accordingly any interference must be justified as necessary and proportionate as balanced against rights of freedom of expression as well as interference in privacy.

- The European Court of Human Rights in recent case law has referred to international law regarding protection of journalists, including Recommendation No. R(2000) 7 on the right of journalists not to disclose their sources of information adopted by the Committee of Ministers of the Council of Europe on 8 March 2000.[309]

The Recommendation[310] includes provisions that domestic law and practice in member States should provide for explicit and clear protection of the right of journalists not to disclose information identifying a source in accordance with Article 10 ECHR and that States should pay particular regard to the importance of the right of non-disclosure and the pre-eminence given to it in the case-law of the European Court of Human Rights311. Disclosure should only be ordered if there is an overriding requirement in the public interest and if circumstances are of a sufficiently vital and serious nature.

- It will therefore be important that the Code of Practice clearly explains in particular that both the issuing authority and the judicial commissioner on review will need to consider the tests of necessity and proportionality against the interference with freedom of expression and the importance given to that right in case law.

Safeguards for information leaving the UK

Disclosure overseas may be made subject to certain restrictions but, for example, clause 41(2) only requires that safeguards are in place "to such extent (if any) as the appropriate issuing authority considers appropriate". Part 3 concerning communications data does not appear to have any specific safeguards in this regard.

Codes of Practice may deal with this in due course. We consider the present provisions could be improved as they provide a very broad and sometimes unfettered discretion; greater legislative clarity is required to create effective operational constraints, for example, on what is meant by the term 'appropriate' in this context. More thought should be given to this when the Bill is drafted.

This is an issue which is currently before the European Court of Human Rights and on which in the European context the CJEU has already raised concerns.[312] We consider that this provision, which leaves the question of what safeguards should apply entirely at the discretion of the issuing authority, risks being ruled unlawful on the ground that it does not

[309] Telegraaf Media Nederland Landelijke Media B.V. and Others v the Netherlands (Application no. 39315/06). 22 November 2012.
[310] Recommendation No. R(2000) 7 on the right of journalists not to disclose their sources of information. www.coe.int/t/dghl/standardsetting/media/doc/cm/rec(2000)007&expmem_EN.asp
[311] The importance of this freedom is also reflected in s. 12(4) of the Human Rights Act 1998.
[312] See Digital Rights Ireland above, and Big Brother Watch and Others v United Kingdom (application number: 58170/13 and 10 Human Rights Organisations v the UK (App No. 24960/15) in the European Court of Human Rights in which the applicants allege that the United States Government has been given access to TEMPORA information.

provide sufficient safeguard against the arbitrary exercise of that discretion. "Future proofing" the legislation strongly points towards providing a higher level of safeguard within the legal framework in this respect.

Oversight

We hope the Government will provide statutory guarantees for the operational independence of the IPC and the Judicial Commissioners who will exercise powers under the proposed warrant authorisation regime.

We also consider the matter of resourcing the IPC should not be left solely to the discretion of the Secretary of State and the Treasury, as the present proposals appear to envisage. We recommend incorporating a role for Parliament in determining the funds the IPC needs to carry out its functions, subject to the availability of public funds.

Summary of recommendations

We recommend:

- Codes of Practice are published alongside the Bill to improve understanding and enable scrutiny of the full legal framework that is proposed.
- The standard of review by judicial commissioners should be clearly explained to make clear that the review of the decision to issue the warrant must include intense scrutiny of whether the warrant is necessary and proportionate.
- Authorisations to access communications data should be made by an independent administrative body rather than a person within the body seeking to use the power.
- The potentially discriminatory impact of bulk surveillance powers aimed at communications abroad should be considered as part of the scrutiny of the draft Bill.
- The power to issue a national security notice should be subject to judicial approval and automatic referral to the IPC for review of how and why the power is being used.
- The safeguards for information leaving the UK should be improved as they provide a very broad and sometimes unfettered discretion; greater legislative clarity is required to create effective operational constraints.
- The framework should incorporate a role for Parliament in determining the funds the IPC needs to carry out its functions.
- The Bill should provide statutory guarantees for the operational independence of the IPC and the Judicial Commissioners who will exercise powers under the proposed warrant authorisation regime.

About the Equality and Human Rights Commission

The Equality and Human Rights Commission is a statutory body established under the Equality Act 2006. It operates independently to encourage equality and diversity, eliminate unlawful discrimination, and promote and protect human rights. The Commission enforces equality legislation on age, disability, gender reassignment,

marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex and sexual orientation. It encourages compliance with the Human Rights Act 1998 and is accredited by the UN as an 'A status' National Human Rights Institution.

Find out more about the Commission's work at: www.equalityhumanrights.com

23 December 2015

Eris Industries Limited—written evidence (IPB0011)

Eris Industries is a London-headquartered company that specializes in providing secure distributed communications systems for large corporates, including a number of the world's leading financial institutions. Our position is that the draft Bill would impinge vital and legitimate business interests of our company. It is also a threat to national security and the well-being of the people of the United Kingdom. If enacted, the draft Bill will present an unacceptable risk to doing digital business here.

We have also, disappointingly, taken positive steps to relocate our base of operations out of London in the expectation that this draft Bill will eventually receive Royal Assent.

We have called on the business community to join us in opposing it and we invite the Committee to undertake a more lengthy and thorough review of these powers before returning its report to the Government.

We note the Committee's request for brevity, given that

> *"The time available for the Committee's inquiry is short, and its focus will be on the contents of the draft Bill rather than more general aspects of policy"*

We find this odd. To begin with, the draft Bill is a statement of policy, and one which

- is highly controversial and almost uniformly opposed by civil liberties advocates;
- is widely opposed by the tech industry, who (after all) know our trade very well; and
- deals with complex matters in relation to which practically every independent expert not affiliated with or in the employ of the security services or the political apparatus disagrees with the Government's approach.

Below we provide our suggestions for how the Committee might go about conducting a more lengthy and thorough review, which we feel is warranted given the scope of this legislation.

1. General

1a. To what extent is it necessary for (a) the security and intelligence services and (b) law enforcement to have access to investigatory powers such as those contained in the Draft Investigatory Powers Bill?

Whether a bill is or is not necessary is a question of whether it will actually address the problem it purports to solve.

It is our opinion that the Government has failed to articulate, with any specificity:

- the specific social ill the draft Bill is to address;
- the existence of credible alternative approaches (such as increased funding for police training, staffing, and equipment); and

- the case for additional surveillance powers, particularly where terrorism is concerned.

We would respond more fully to the full list of the questions posed in your Call for Evidence, e-mail notice of which we received on 1 December 2015 (11 days ago, leaving 6 to respond in time for the very tight deadline of 21 December).

However, evidence on this matter is rather thin on the ground. The secret nature of existing mass surveillance programmes means that the public, business, and civil society alike are quite unable to provide adequate scrutiny of the Government's claims of necessity.

We cannot opine on what we do not know. It is therefore difficult to determine whether these powers are necessary. This alone should be troubling.

Even if we could show that the powers are necessary, there is the other matter that the Government's chosen course of action is fraught with risk. The Government has either downplayed or completely failed to address the serious dangers posed by weakening data security and increasing data retention.

With this draft Bill, the Government is asking vast swathes of British and international business to retain truly incomprehensible quantities of data on its behalf – a year's worth of activity of every communication into and out of, and of every man, woman and child in – the country. The Government furthermore wants industry to also preserve the means to access these communications on an ongoing basis, if ordered to do so, by removing electronic protection[313] from this data – "in extremis," we are told.

Data which is retained is data which can be stolen. A communication which has its electronic protection removed for the Home Secretary is a communication which has also had its electronic protection removed from the viewpoint of state-sponsored hackers in countries known to sponsor such activity, which shall remain nameless in this correspondence.

Every window we give our security services is a back door for our enemies. We should not therefore be asking ourselves whether these powers are necessary. We should be asking ourselves whether these powers, and the reduction of data security they will give rise to, are dangerous and, on balance, will pose a greater risk to our national security and economic competitiveness than the alternative.

As to the facts to which we can prove in our role as public critics of this policy, they are as follows:

- bulk collection and interception powers, where tried and where the results are known, has failed utterly to stop terrorism[314] (or, where paired with mainstream law

[313] See the draft Bill, s. 189.

[314] McLaughlin, Jenna: "U.S. Mass Surveillance Has No Record of Thwarting Large Terror Attacks, Regardless of Snowden Links." *The Intercept*, 17 November 2015. https://theintercept.com/2015/11/17/u-s-mass-surveillance-has-no-record-of-thwarting-large-terror-attacks-regardless-of-snowden-leaks/ Accessed 11 December 2015.

enforcement, has resulted in wanton and serious breaches of citizens' rights against unreasonable searches and seizures and violations of due process rights[315]);

- terrorists are getting and do get through, and often they do so without using sophisticated encryption or other technologies the Government proposes to regulate (see, e.g., s. 189 of this draft Bill). Neither the Charlie Hebdo murders in January 2015, nor the November 2015 attacks on Paris, nor the December 2015 attacks on California, nor indeed the 9/11 attacks involved the use of electronic protection of any kind for the perpetrators' communications;

- cryptographic tools which would render communications invisible to the Government are free and open-source, meaning terrorists and serious criminals could easily migrate to these platforms after the draft Bill received Royal Assent while leaving the British people (and their data) vulnerable for the reasons described above; and

- many of the arguments the Government has made regarding the feasibility of implementing the draft Bill have been comprehensively debunked,[316] time and again, over the last 20 years by the world's leading academic cryptographers and data security professionals.

In other words, the draft Bill does not solve many, if any, of the problems it is purportedly meant to address. Furthermore its provisions are known to be problematic from an implementation standpoint. And to ask for more bulk collection where bulk collection has clearly already failed is like failing to find a needle in a haystack – and deciding the solution is more hay.

Given the short timeframe the Committee has to conduct this consultation, all there is left for us to do is implore the Committee to immediately contact independent cryptography and data security experts who have no connection to the security services. Some, such as

---

If we look to jurisdictions with similar programmes but which have had the benefit of involuntary public interest disclosures, such as the United States, evidence points to the fact that these programmes do not, in fact, work. I direct your attention to leaks obtained by the *Intercept* news website, linked above, which show that in the case of the American government – by its own admission – bulk collection has

> *"no record of thwarting large terror attacks, regardless of Snowden leaks…Even before Snowden, the NSA wasn't able to provide a single substantiated example of its surveillance dragnet preventing any domestic attack at all."*

We invite the British government to prove that its bulk collection programmes are any more effective than that of their American counterparts. In the absence of such proof, the available evidence compels us to arrive at the conclusion that these programmes do not work.

[315] Shiffman, John and Cooke, Christina. "United States directs agents to cover up program used to investigate Americans." Reuters, 5 August 2013. http://www.reuters.com/article/us-dea-sod-idUSBRE97409R20130805 Accessed 11 December 2015.

[316] Abelson, Anderson, Bellovin, Benaloh, Blaze, Diffie, Gilmore, Green, Landau, Neuman, Rivest, Schiller, Schneier, Specter, Weitzner. *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications.* Technical report of the MIT Computer Science and Artificial Intelligence Laboratory, 6 July 2015. https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf

Graham Cluley, are based in the UK. Many others, such as the authors of the work referenced in footnote 4, may be found in the United States.

If the Committee were to follow this course of action, it would find itself much better advised than the Government.

We offer no further comment.

Facebook Inc., Google Inc., Microsoft Corp., Twitter Inc., Yahoo Inc.—written evidence (IPB0116)

INTRODUCTION

1. National security is an important concern for Governments. Governments have a responsibility to protect people and their privacy. We believe a legal framework can protect both. Our companies want to help establish a framework for lawful requests for data that, consistent with principles of necessity and proportionality, protects the rights of the individual and supports legitimate investigations.
2. As members of the Reform Government Surveillance (RGS) coalition (www.reformgovernmentsurveillance.com), we believe the best way for countries to promote the security and privacy interests of their citizens, while also respecting the sovereignty of other nations, is to ensure that surveillance is targeted, lawful, proportionate, necessary, jurisdictionally bounded, and transparent. These principles reflect the perspective of global companies that offer borderless technologies to billions of people around the globe.
3. The actions the UK Government takes here could have far reaching implications – for our customers, for your own citizens, and for the future of the global technology industry. While we recognize the UK Government has made efforts to develop a clear, comprehensive and modern legal framework, we would offer several important considerations that shape our view of the Bill:
    - User trust is essential to our ability to continue to innovate and offer our customers products and services, which empower them to achieve more in their personal and professional lives.
    - Governments' surveillance authorities, even when transparent and enshrined in law, can undermine users' trust in the security of our products and services.
    - Key elements of whatever legislation is passed by the UK are likely to be replicated by other countries, including with respect to UK citizens' data.
    - Unilateral imposition of obligations on overseas providers will conflict with legal obligations such providers are subject to in other countries.
    - An increasingly chaotic international legal system will leave companies in the impossible position of deciding whose laws to violate and could fuel data localization efforts.
4. We appreciate the opportunity to consult on the Bill. To that end, we advance a number of issues that we believe are important to serve UK citizens and the citizens of other nations, while ensuring that citizens' human rights and privacy rights are protected. This includes ensuring the Bill satisfies ECJ scrutiny and also builds greater legal certainty and consistency for the proposed measures.

PRIMARY CONCERNS

1. **Extraterritorial Jurisdiction (ETJ)**

a) **Conflict of laws:** As noted earlier, we anticipate that other countries will emulate what the UK does here. Unilateral assertions of extraterritorial jurisdiction will create conflicting legal obligations for overseas providers who are subject to legal obligations elsewhere. The UK Government understood this in 2009, when the Home Office Consultation 'Protecting the Public in a Changing Communications Environment' stated that RIPA did not apply to overseas providers. Conflicts of laws create an increasingly chaotic legal environment for providers, restricting the free flow of information and leaving private companies to decide whose laws to violate. These decisions should be made by Governments, grounded in fundamental rights of privacy, freedom of expression, and other human rights.

   If the UK legislation retains authority to reach extraterritorially, the Bill should consistently and explicitly state that no company is required to comply with any notice/warrant, which in doing so would contravene its legal obligations in other jurisdictions. Enforcement obligations should also take this into account. Notwithstanding our position, currently there is confusion: the context section of the Bill overview document states, "Enforcement of obligations against overseas CSPs will be limited to interception and targeted CD acquisition powers". This is not what the Bill itself says.

b) **International framework:** We agree with the recommendation of Sir Nigel Sheinwald and others that an international framework should be developed to establish a common set of rules to resolve these conflicts across jurisdictions. These rules should facilitate more efficient requests in cases that provide adequate protections for user privacy. There are indications in the legislation that the UK Government has identified an approach that could work. Though interception is generally prohibited, for example, the Bill permits interception in the UK when it is done “in response to a request made in accordance with a relevant international agreement.” If the UK Government’s authority should have unlimited application overseas, it is unclear why the UK Government believes other countries’ authorities should only extend into the UK pursuant to an international agreement. Instead, a better approach would be to condition the extraterritorial application of UK law to situations where it is done pursuant to an international agreement that permits it, and furthermore resolves conflicting obligations in the other country.

c) **Service of warrants on overseas providers:** The Bill permits warrants to be served on companies outside the UK in a number of ways, including serving it on principal offices within the UK. Despite ETJ language, this presents a risk to UK employees of our companies. We have collective experience around the world of personnel who have nothing to do with the data sought being arrested or intimidated in an attempt to force a overseas corporation to disclose user information. We do not believe that the UK wants to legitimize this lawless and heavy-handed practice.

2. **Technical impositions:**

a) **Clarity on encryption:** The companies believe that encryption is a fundamental security tool, important to the security of the digital economy as well as crucial to ensuring the safety of web users worldwide. We reject any proposals that would require companies to deliberately weaken the security of their products via

backdoors, forced decryption, or any other means. We therefore have concerns that the Bill includes *"obligations relating to the removal of electronic protection applied by a relevant operator to any communication or data"* and that these are explicitly intended to apply extraterritorially with limited protections for overseas providers. We appreciate the statements in the Bill and by the Home Secretary that the Bill is not intended to weaken the use of encryption, and suggest that the Bill expressly state that nothing in the Bill should be construed to require a company to weaken or defeat its security measures.

b) **No business should be compelled to generate and retain data that it does not ordinarily generate in the course of its business**. Some language under the retention part of the Bill suggests that a company could be required to generate data – and perhaps even reconfigure their networks or services to generate data – for the purposes of retention.

3. Judicial authorization:

a) **Judicial review standard:** As recommended by David Anderson QC, Governments should not be able to compel the production of private communications content absent authorization from an independent and impartial judicial official. While we believe the Bill's 'double lock' represents an important step in the right direction, there remains room for improvement. The "judicial review" standard should be clarified to ensure that the judge reviews the actual merits of the matter, and not just the process by which decisions and actions were taken by the authorizing secretary. To truly serve as a second lock, this function must not just assess the rationality or reasonableness of the ministerial decision, but ensure that investigatory warrants under the Bill will withstand the full scrutiny of a court.

b) **Applicability:** we believe that judicial authorization should be applied to a broader set of authorities and also be extended to national security notices, maintenance of technical capability orders, and modifications to equipment interference warrants which have been issued to the Chief of Defence Intelligence and intelligence services.

4. **Bulk collection**

a) **Explicit language:** As set forth in the Reform Government Surveillance principles, surveillance laws should not permit bulk collection of information. The principles require that the Government specifically identify the individuals or accounts to be targeted and should expressly prohibit bulk surveillance. The word "bulk" can be ambiguous. We understand from David Anderson QC's report that, in the UK, bulk warrants allow a specific communications channel external to the UK to be specified due to the link with a specific national security or serious crime threat. It is then filtered and searched for identifiers. In terms of setting international precedent, we therefore suggest that the Bill be more explicit in the language it uses, highlighting that any collection should be pursuant to a specific identifier.

b) **Minimization provisions:** We also believe that the general safeguards sections should explicitly include 'minimization' provisions, ensuring that only the necessary and proportionate amount of data is obtained, analyzed and retained. All other data should be destroyed.

5. **Transparency and Clarity**

a) **Elimination of Vague and Confusing Language:** As David Anderson QC highlighted in '*A Question of Trust*', legislation on surveillance powers should be written in such a way that the intelligent reader can understand the surveillance powers possessed by the Government, and how, where and by whom they are used. Legislation or practice that is wide-reaching and vague harms the ability of the users and companies to understand government surveillance. It also impacts on the ability of formal and informal oversight mechanisms, including NGOs, to carry out their function effectively. There are many aspects of the Bill which we believe remain opaque: judicial authorization; the extent of the obligations on companies outside of the UK; the confusing messages about the extent to which there is an obligation to produce material that can be read versus the Government's statement about the Bill not prohibiting encryption; and the obligations on technical capability. We outline additional suggestions in the document. We urge the Joint Committee and the Home Office to do all that it can to ensure that the whole Bill is written clearly and unambiguously.

b) **User notification:** As a general rule, users should be informed when the Government seeks access to account data. It is important both in terms of transparency, as well as affording users the right to protect their own legal rights. Our users range from individual consumers to large media organizations to large public sector entities. Even where the Government establishes a need to obtain certain information, it does not necessarily deprive users of other rights they may have, and knowledge of the request is essential to their ability to advance those rights. While it may be appropriate to withhold or delay notice in exceptional cases, in those cases the burden should be on the Government to demonstrate that there is an overriding need to protect public safety or preserve the integrity of a criminal investigation.

c) **Warrant recipient:** We welcome the Bill's clarification that warrants must be both "necessary and proportionate." However, once there is a determination that a warrant is necessary, the question should then be to whom the warrant should be directed. It is our view that the same standard – "necessary" – should be applied when evaluating this question. In many cases, the Government can (and often does) obtain the information directly from the users themselves. When that is not possible, the Government should seek the information from the most proximate source with access to the data. An obvious example of this involves enterprise cloud customers. Even as private sector and public sector entities transition to the cloud, they remain in complete control of their own data. Before they moved data off of their own servers and onto the servers of large cloud providers, Governments would go to them for their data or the data of their employees. There is no reason Governments cannot continue to do the same after these organizations transition their data to the cloud. This is an area where the UK can lead the rest of the world, promoting cloud adoption, protecting law enforcement's investigative needs, and resolving jurisdictional challenges without acting extraterritorially.

d) **Overseas provider standing:** Overseas providers should have a legal right to seek legal advice and raise complaints with the Commissioner without either committing a disclosure offence or accepting jurisdiction. There should be the possibility for judicial commissioners to request amicus briefs from affected providers.

e) **Clarity on urgent provisions, e.g. approval of warrants issued in urgent cases**. The term "urgent" is not defined in the Bill. Clarity on this term - which other countries may seek to emulate and even abuse - is important.

6. **Computer Network Exploitation**:

a) **Risk to user trust:** The ultimate test we apply to each of the authorities in this Bill is whether they will promote and maintain the trust users place in our technology. Even where these authorities do not apply to overseas providers like our companies, we are concerned that some of the authorities contained in the Bill, as currently drafted, represent a step in the wrong direction. The clearest example is the authority to engage in computer network exploitation, or equipment interference. To the extent this could involve the introduction of risks or vulnerabilities into products or services, it would be a very dangerous precedent to set, and we would urge your Government to reconsider.

b) **Network integrity and cyber security requirements:** There are no statutory provisions relating to the importance of network integrity and cyber security, nor a requirement for agencies to inform companies of vulnerabilities that may be exploited by other actors. We urge the Government to make clear that actions taken under authorization do not introduce new risks or vulnerabilities for users or businesses, and that the goal of eliminating vulnerabilities is one shared by the UK Government. Without this, it would be impossible to see how these provisions could meet the proportionality test.

We are happy to follow up in writing with any queries you have on this written evidence, and undertake to answer, via email, within 24 hours including during the holiday period. We are also happy to provide specific drafting comments, should you wish these.

Facebook Inc.

Google Inc.

Microsoft Corp.

Twitter Inc.

Yahoo Inc.

21 December 2015

F-Secure Corporation—written evidence (IPB0118)

About F-Secure Corporation and its interests in the Bill

1) F-Secure is a cyber security and privacy software company which has been operating for nearly 30 years – from just after the advent of the first computer virus. Headquartered in Finland, our company operates globally and has a presence in the UK as well. Originally, an anti-virus software company, in recent years, F-Secure's portfolio has expanded to include cyber security services; giving consultancy to large organisations on how to keep their online assets protected. A considerable concern for these corporations is protection not only from well-resourced criminals but also from nation-states, governments and military organisations that have, in recent years, increasingly resorted to hacking methods.

2) The proposed Investigatory Powers Bill is a clear statement of intent on behalf of the British Government to engage in activities that many foreign businesses and non-nationals would regard as a threat to their cyber security and privacy worth protecting against.

3) Among F-Secure's portfolio of security and privacy-enhancing products is a tool called Freedome – a hybrid virtual private network (VPN) solution that provides the user with virtual locations, measures against tracking attempts and protection against malicious websites. VPNs create an encrypted tunnel through which a user's data is transmitted to the other side of the internet, safe from the prying eyes and ears of eavesdroppers, immune to attempts to exploit the access network the user has connected their device to. Evidence shows there is a pronounced need for such a service when connecting through public Wi-Fi hotspots. Several documented cases[317] demonstrate how easy it is to steal users' credentials from unencrypted connections. Importantly, this anonymity and protection also gives users in undemocratic countries the freedom to use the internet and exercise the right to free speech without fear of repercussions.

4) The introductory guide provided alongside the draft Bill refers to 'Communications Service Providers' (CSPs). The terms has also been used throughout the Committee hearings. However, the term is nowhere to be found in the draft Bill itself. Instead, the term 'telecommunications operator' is used. In our understanding, 'telecommunications operator' is a much narrower term than what is implied by CSP in the guide.

   The vague nature of the definition of CSPs means that F-Secure has difficulty in establishing whether the Bill would introduce new obligations on us as a company. As a foreign technology company (which most technology companies are to Britain), further information and greater clarity would be needed as to the applicability of the law on services that our industry provides.
   In addition, there is ambiguity in the Bill as to whether strong end-to-end encryption would in the future be tolerated under UK legislation and whether the government would require technology companies to introduce backdoors in their software products and service production platforms. F-Secure strongly opposes such requirements. As one of the most

[317] Including *The Great Politician Hack* conducted by F-Secure. This is the project which Lord Strasburger declared his interest in during the expert witness hearing involving F-Secure on the 21st December 2015. https://www.youtube.com/watch?v=eyNjyTiIRvI

established security companies in the world, it is our duty to explain the practicalities of these actions and the likely outcomes.

In answer to questions posed by the Committee…

Is the legal framework such that CSPs (especially those based abroad) will be persuaded to comply?

As a good corporate citizen, F-Secure has a zero tolerance stance towards criminal activity and terrorism. We want to help law enforcement agencies in their invaluable role of keeping society safe and secure. As such, we are open to warrant-based requests. However, it would be essential that the process is transparent and strong checks and balances are in place to protect our business (and our brand identity as a trusted partner), our customers and even the authorities from misuse of power and mission-creep.

As a Finnish company, F-Secure is subject to local laws, meaning all warrants would potentially have to pass through our own court system (which values privacy highly). Many VPN and communications service providers which sell their products in the UK are in a similar position, in that they are not headquartered in the UK. This is where the difference between targeted and bulk collection schemes will become apparent. The majority of technology companies will, like us, wish to help the authorities in stopping criminal behaviour. The quickest and cheapest approach would be to enter into a voluntary agreement to assist as necessary, building a relationship of trust. This will have a more favourable and swifter outcome for the government agencies seeking data, but they will only benefit from this relationship if the data requested is targeted. Bulk collection oversteps the mark and makes companies, foreign governments and legal systems uncomfortable. Few companies will enter into a voluntary agreement if they believe the powers being wielded by the state are disproportionate and unnecessary.

If British law is changed to compromise our product and brand reputation, further internal discussions will need to take place as to our strategy in the UK. We are not the only technology company with these reservations. In October, 74 technology companies joined with us to sign an open letter[318] to the Government (published in *The Times* on the 29th October) outlining our concerns with this Bill and the damage it could do to the UK technology industry as a whole. Just recently, Apple's CEO Tim Cook defended their choices with regard to encryption[319].

Are the powers sought workable and carefully defined?

- **Are the technological definitions accurate and meaningful (e.g. content vs communications data, internet connection records etc.)? Does the draft Bill adequately explain the types of activity that could be undertaken under these powers? Is the wording of the powers sustainable in the light of rapidly evolving technologies and user behaviours? Overall is the Bill future-proofed as it stands?**

The Bill introduces a totally new concept of 'Internet Connection Records'. To the best of our knowledge, the collection of ICRs is something that the telecommunications operators have not done before on an infrastructure-wide fashion. The operators would be required to install new equipment and procedures to collect, store and search the data.

[318] Full text of the letter: http://news.f-secure.com/Openletter?elqTrackId=7B454B19B7BCE1D0E8E4CBB577BA9A15&elq=00000000000000000000000000000000&elqCampaignId=&elqaid=1320&elqat=2

[319] http://techcrunch.com/2015/06/02/apples-tim-cook-delivers-blistering-speech-on-encryption-privacy

F-Secure would like to draw the committee's attention to the fact that the data would not only be voluminous but also highly sensitive in nature. The operators would be required to build elaborate cyber security protections to safeguard the data, limit access to the store and audit the system's use. Further complicating the task would be the fact that the system would need to be online and highly networked as it would vacuum in all the ICRs from highly distributed access networks throughout the country. The system would be prone to breaches and would likely make the operators a target for criminal attacks and computer network exploitation (CNE) operations conducted by foreign governments.

The Bill appears to avoid the technical detail of how access to bulk datasets will be acquired. Much has been spoken of the Government's wish to ban encryption, compromise encryption systems or provide backdoors. It is important that this is highlighted, as it is impossible to ban encryption for two reasons: firstly, it is a branch of mathematics (and therefore an expression of free speech). Encryption can no more be banned than Pythagoras' theorem. Secondly, it is already in use. It is taught in universities and on computing courses. Many people know how to create encrypted technologies that banning it will not stop it existing. Even if a ban were brought into law, the criminals will still not be law-abiding and will circumvent the law, while the innocent masses will now no longer have the protection of encryption when shopping online, conducting financial transactions and the like. As individuals, our expectations for secure eCommerce, eGovernment and personal privacy make it necessary to have access to strong cryptography in terms of encryption, authentication and integrity enforcement. There is a saying about locks only keeping out honest people. The same applies to weakened cryptography.

It has been suggested that a 'backdoor' could be provided to government agencies to access encryption systems. F-Secure opposes any attempts to undermine online security through creating vulnerabilities in otherwise secure systems. Once a vulnerability is introduced, it will only be a matter of time before it will be detected and exploited by criminals. Encrypted systems would become a highly prized target, as the vulnerability would then be known to exist. These online criminals include hacking teams backed by nation states – some of which are looking for targeted information, some of which are bulk collecting data for possible use in the future.

Within the Bill, there are provisions to provide services with 'Bulk interception' capabilities and the ability to conduct targeted and bulk 'equipment interference'. From a technology or operational point of view, the Bill does little to explain how these powers would be used in actuality.

Bulk interception would possibly require the cable owners and operators of a switching or router infrastructure to provide authorities with raw access to cables or data streams. Such industrial scale eavesdropping – or tapping – of communication is likely expose thousands or even millions of end users' data to mass surveillance. Equipment interference, on the other hand, is what all hackers in the world would regard as 'attacks', computer intrusions, introduction of backdoors and artificial weakening of encryption. Intelligence organisations and military refer to these actions as CNE.

With regard to the bulk datasets, many questions are raised as to how this data can be provided in near real-time to a number of law enforcement authorities, while maintaining the security of the data. As the data would have to reside online in one form or another to allow this access, its vulnerability to hacking is heightened.

Ultimately, this Bill is positioned as a means by which the British Government will protect the British public from criminal activity and terrorism. Unfortunately, F-Secure sees that the

contrary will be achieved. By weakening online security, every person in the UK is open to attack from criminal elements who could gain access to personal data and financial information.

Are there sufficient operational justifications for undertaking (a) targeted and (b) bulk interception?

This Bill is essentially a list of everything which Britain's intelligence agencies would like for Christmas. Even so, remembering the extremely fast-paced schedule with which such a complex Bill is being rushed through the Parliament, there needs to be significant consideration as to whether it should be done. Technological ability alone cannot be the judge of that. As it is already being considered whether this Bill needs to be scrutinised periodically in the future (e.g. once in each parliament), a more prudent approach would be to conduct targeted collection of data and assess if this has indeed produced the limitations the government agencies are concerned about. This will avoid disruption of potential communications service provider businesses in the UK which will be viewed with suspicion when a superpower government is forcing the bulk collection of data.

Curiously, while we provide a secure, anonymous and privacy-enhancing communications service, we have received only a handful of requests for information from law enforcement agencies throughout the world – none from the UK this year. From our perspective, there appears to be a disconnect between the stated claims from law enforcement officials that the internet has 'gone dark', when there have been no serious efforts to acquire this information.

It is for this reason that we oppose the bulk requests for customer information or communications data. It is curious that there is a thirst to jump to collect data in bulk when more targeted and privacy-respecting methods have not been utilised in full.

Additionally, handing over information in bulk would seriously undermine our reputation as an ethical and trustworthy company (essential for a security provider) and make us a target for unwanted criminal and intelligence collecting activity conducted by various threat actors around the globe.

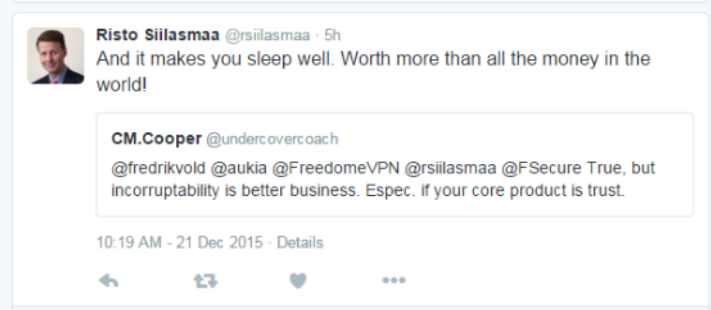


Figure 1 A quote from F-Secure's chairman Risto Siilasmaa's Twitter message today about the need for a Cyber Security company to be trustworhy.

Are the proposed safeguards sufficient for the secure retention of material obtained from interception?

We believe that without specific consent for data collection, the government should do the right thing by putting in place limits which will respect the fact that people have an expectation of privacy.

With the Freedome VPN, It is worth noting that any data logged would be limited by the very nature of the technology. The encrypted tunnel which a VPN creates means that we

guide our customers to the internet through a node of their choosing (which can be in one of 25 countries). Once on the internet, we are unaware of their activities. It is the equivalent of telling the police in which direction the car they are after went. A lot of investment would be required for gathering even this minimal amount of information. Currently this is something we do not collect, and wish to continue doing so. Interestingly, we have received no feedback from law enforcement agencies anywhere in the world that would suggest that our VPN tool has hindered criminal investigations or their resolution.

We would be reticent to store material obtained by targeted or bulk collections. This is due to the practicalities of storing this highly valuable data. The content of these collections would make the database a target for multiple hacking organisations (including, but not limited to, criminal gangs, hactivists, terrorist organisations and nation states). As a security company which recently sold a cloud-based content storage company, we are fully aware of the costs and man-hours required to develop and maintain a secure system, especially when considering the resources of nation-state hacking groups. Few other companies hold our heritage in cyber security, so there is a question of whether they would fully understand and be able to manage the heavy burden of keeping this data secure.

No system is full-proof. We urge the government to carefully consider the people they are putting at risk by storing this data in multiple silos. Whether or not a British citizen uses the internet, their details will be on these databases. Should the databases be successfully hacked, there is the potential that every person in the UK is compromised and a potential victim of identity fraud or worse. This should be a major consideration of the Committee.

Are the definitions of content and communications data (including the distinction between 'entities' and 'events') sufficiently clear and practical for the purposes of accessing such data?

From the network technology point of view, the definitions are not practical to allow for different courses of action to take place dependant on whether the data is classed as entity or event. There is a significant amount of crossover between entities and events. At the moment of collection and data extraction (interception), it will be difficult or impossible to utilise such divisions. These will only become apparent at later stages when the data is examined. If this was the intent, these definitions may turn out be useful.

Is accessing Internet Connection Records essential for the purposes of IP resolution and identifying of persons of interest? Are there alternative mechanisms? Are the proposed safeguards on accessing Internet Connection Records data appropriate?

With Internet Connection Records, it is important to remind the Committee that the access network level logs give a poor signal to noise ratio. For instance, in the case of most of the websites, the only thing logged would be that the user's computer connected to Akamai's, Microsoft's, Amazon's or Google's cloud services. These are called Content Delivery Networks (CDNs) and they provide an added level of technology abstraction between the end user and the actual service that the user accesses. Most of the mobile apps and many cloud-based services also do constant polling towards these services (several times a minute) and will not necessarily reveal whether the activity was human-initiated or conducted by the background activity of the app. Lastly, a user of VPN services such as Freedome would only be seen as connecting to the VPN gateway after which the true destination of the traffic would be hidden from the ICRs point of view.

21 December 2015

Mr Peter Gill—written evidence (DIP0008)

Oversight

This submission is made in my personal capacity as a Senior Honorary Research Fellow at the University of Liverpool.

1. What are the advantages and disadvantages of the proposed creation of a single Judicial Commission to oversee the use of investigatory powers?

1.1 This draft Bill represents the first time that intelligence control and oversight issues have been addressed holistically; the structure of commissioner/tribunal was first initiated in 1985 and has 'just growed' since then through 1989, 1994, 1997, 2000. RIPA may have brought comprehensive legislation for the first time with respect to the *authorisation* of covert intelligence (required to ensure compliance with the Human Rights Act 1998) but it retained the essentially piecemeal system for *oversight* that had developed to that point. The post-Snowden inquiries clearly indicate that 'Public confidence in the acquisition and retention of data rests on the credibility and practicality of the legal and oversight frameworks that govern it.'[320]

1.2 The main advantage of the draft Bill is that it merges the existing three commissioners and proposes that the Investigatory Powers Commissioner (IPC) is defined functionally, rather than in terms of specific agencies (as the Intelligence Services Commissioner is currently). The draft Bill covers the entire community of those empowered to conduct covert investigations and will complement the work of the Intelligence and Security Committee (ISC) that will continue to oversee policy, administration, expenditure.

1.3 The main disadvantage of the proposal in the Bill is that the IPC conducts both authorisation and oversight: this combines two functions that should be kept separate. With respect to authorisation the new IPC is to apply judicial review principles in assessing the necessity and proportionality of warrant requests. Clearly the draft bill is an improvement on the current authorisation situation because it involves judges in the approval of warrant applications and thus adds a judicial dimension to the 'political' decision made by ministers. This is appropriate because the determination as to whether an application passes the triple test of legality, necessity and proportionality as required by the Human Rights Act is, finally, a legal question.

1.4 However, 'oversight' requires a much broader set of expertise. This is recognised in the Bill to the extent that the IPC will be provided with judicial, official, legal and technical support[321] but the staff of an independent oversight office would need a greater emphasis on investigative and analytical skills; in some ways mirroring those of the agencies themselves.[322] Perhaps such a staff could be assembled under the structure envisaged in the draft Bill but it would not enjoy the required degree of independence if it were headed by a judicial Commissioner who was also responsible for the other commissioners when authorising warrants. This looks too much like the judges being asked to 'mark their own homework' and would fail the test of being *seen* by the public to be independent oversight.

1.5 This draft Bill has drawn extensively on the post-2013 reviews conducted by ISC, Anderson and RUSI. The ISC considered several proposals for reform but its report

[320] RUSI, 2015, *A Democratic Licence to Operate: Report of the Independent Surveillance Review*, p.73, 4.1.
[321] Draft Investigatory Powers Bill, clause 176, explanatory notes, p.54.
[322] cf. RUSI, 2015, p.91, 4.82.

recommended that ministers should remain solely responsible for authorising warrants and that the responsibility for oversight should remain with the three commissioners and themselves with their enhanced powers under the Justice and Security Act 2013.[323] Both Anderson and RUSI, however, were more concerned at the complexity and lack of clarity in the existing oversight system, for example,

> 'There is certainly a problem of trust in the system of oversight, and particularly the lack of popular visibility of the oversight arrangements that currently exist. A clear and transparent new legal framework and a more coherent, visible and effective oversight regime should be the basis for a public discussion about the appropriate and constrained power the British state should have to intrude into the lives of its citizens. This would be the essence of a new deal between citizen and government.[324]

1.6 Further, Anderson and RUSI both recommended not only that judicial authorisation for covert investigations be introduced but also that the existing commissioners be combined in a single office and this idea has been taken up in the draft Bill. With respect to his proposed Independent Surveillance and Intelligence Commission (ISIC), Anderson concluded:

> 'I have considered whether it would be difficult to combine the judicial authorisation function and the inspectorate in a single organisation, and concluded that it would not. A precedent already exists, in the form of the OSC whose six judicial Commissioners, three Assistant Commissioners and eight Inspectors all report, along with the secretariat, to the Chief Surveillance Commissioner ... Whilst the judicial function is obviously a distinct one, there is considerable benefit in dialogue: the Judicial Commissioners could advise the inspectorate on matters to look out for on their inspections, and the inspectors could in turn suggest that a warrant be referred back to the Judicial Commissioners if they formed the impression that it was not being implemented as it should be, and that the Judicial Commissioners might wish to consider modifying or cancelling it.'[325]

1.7 It is not 'difficult' to combine these functions, as Anderson says, but the real question is whether it is *desirable*, especially given what he acknowledges as the 'distinct' nature of the judicial authorisation function. Indeed, Anderson's Model B for the organisation of the new office provides for the Chief Judicial Commissioner with responsibility for authorisations to be separate from the non-judicial Chief Commissioner in charge of the inspectorate.[326]

1.8 RUSI's recommendation is more explicit on this point:

> 'The judicial commissioners in charge of the authorisation of warrants *should not be* part of a new National Intelligence and Surveillance Office nor should they be based in a government department, but alternative office facilities should be sought so that the commissioners are accessible but remain independent.'[327]

This is crucial and is the reason why there should be a clear separation between the *direction/control* of covert investigations (in the hands of ministers and officials) and their *authorisation* by judicial commissioners, on the one hand, and the *oversight* of covert

---

[323] ISC, *Privacy and Security: a modern and transparent legal framework*, 2015, pp.73-81.
[324] RUSI, 2015, p.103, 5.30.
[325] Anderson, 2015, *A Question of Trust: report of the investigatory powers review*, p.281, 14.98.
[326] Anderson, 2015, p.373, Annex 18.
[327] RUSI, 2015, p.111, added emphasis.

activities based on 'audits, inspections and investigations' on the other.[328] Therefore, the RUSI recommendation is nearer to what is required for the structure not only to be more effective but, crucially, to be seen to be more effective,

> 'A NISO should have an office based outside of the Whitehall departments, have a public profile and be led by a senior public official. The new organisation should be staffed by appropriate persons with technical, legal, investigative and other relevant expertise (for instance in privacy and civil liberties).'[329]

1.9 These 'audits, inspections and investigations' should cover comprehensively the field of intelligence.[330] In determining its work priorities, it would be useful for the Commission to discuss work agendas with the ISC to prevent duplication and obtain maximum leverage on the scarce resources available for oversight. For example, one of the major controversies in the wake of the Snowden file releases is the extent of 'bulk collection' which constitutes a potentially massive invasion of privacy but the effectiveness of which is doubted by some. The IPC could make a major contribution by subjecting to continuing audit questions such as whether the agencies are drowning in data when what they really need is an increase in analytical capacity and skills.

1.10 One of the criticisms of the oversight structure as it has developed since 1985 is its fragmentation and the draft bill certainly seeks to address that; therefore, while the new judicial authorisation arrangements should be separate from those for oversight, there should certainly be dialogue between the two.

2. Would the proposed Judicial Commission have sufficient powers, resources and independence to perform its role satisfactorily?

2.1 *Complaints*: the draft Bill envisages the continuation of the practice whereby members of the public who believe they have been the victim of an abuse of investigatory powers may lodge a claim with the Investigatory Powers Tribunal (IPT). By definition, people will normally remain unaware of being subject to covert surveillance, authorised or not, and RUSI pointed to the systemic weakness of the IPT in that errors only come to light after claimants make an application to the tribunal.[331] To some extent this systemic weakness is addressed by the new provision for 'error reporting' (cl. 171). But IPT has minimal investigatory resources and relies for most of its information on that provided by the agencies. This is clearly inadequate.

2.2 Experience elsewhere (e.g. Belgium, Canada, Netherlands) is that extra-parliamentary oversight bodies find that the investigation of specific complaints provides a detailed insight into agencies' *modus operandi* and record-keeping and thus complements their other review activities. In turn, the broader oversight mandate of these bodies enables them to exercise good judgment as to the significance or otherwise of complaints that are made. Therefore the present situation would be improved by the IPC becoming the recipient for public complaints, investigating them and, if appropriate, making recommendations to the IPT or acting as a 'friend of the court' in any subsequent hearing (see further 4.2 below).

---

[328] Draft Bill, cl.169.
[329] RUSI, 2015, pp.112-3.
[330] cf. Anderson, 2015, pp. 96-97 regarding a 'more general supervisory power over the activities of the security and intelligence agencies'.
[331] RUSI, 2015, p.94, 4.94.

2.3 *Employees ethical concerns*: Since 1987 the Staff Counsellor has acted as an independent outlet for employees of the three agencies with ethical concerns about their work or agencies' activities. S/he makes at least an annual report to the Prime Minister but the role is non-statutory and little is known in public as to how effective this has been or how employees view the office. As with public complaints, employees should be able to contact the IPC directly and hearing their concerns would inform the IPC's office regarding difficult issues. Clearly, in the post-Snowden world, a robustly-independent yet confidential outlet for employees is required in order to minimise the risk of damaging disclosures.

2.4 *Reports* of the IPC into investigations should be made public insofar as possible. The public presentation of annual and specific reports would secure a public face for the IPC which, together with the ISC's raised profile, would assist in the key role of public education in this most arcane of government functions. In pursuance of the principle of a cohesive framework for oversight, if confidential annexes are required (or entire reports produced that cannot be made public) then they should be sent simultaneously to the PM and the ISC. If reports are made initially to the PM, then there should be a time limit within which the report must be laid before Parliament.

2.5 *Improved public education*.[332] Both RUSI and Anderson refer to the need for the new oversight structure to have a 'public face'.[333] Whatever the disposition of the law, there is a crucial political task for governments and intelligence oversight bodies to explain the *reality* of current security surveillance when the *potential* is clearly so vast and threatens public trust. This function should be added explicitly to the mandate for the IPC.

3 Are the appointment and accountability arrangements for Judicial Commissioners appropriate?

3.1 Given the importance of the new structures for authorisation and oversight being seen to be independent, there is a strong case for the ISC having an advisory role in the appointment of the IPC head.[334] Since the ISC has had public meetings with the heads of the three agencies and several in connection with its own Privacy and Security inquiry, it would be helpful if they interviewed proposed appointees in public.

4 Are the new arrangements for the Investigatory Powers Tribunal including the possibility of appeal adequate or are further changes necessary?

4.1 Quite rightly, clause 180 of the draft Bill introduces a right of appeal from the Investigatory Powers Tribunal (IPT) and clause 171 makes provision for victims to be informed of what are agreed by the IPC and IPT to be 'serious errors' in the use of investigatory powers, including that they have the right to bring a claim to the IPT. The bill continues the provision by which IPT may ask for assistance from judicial commissioners (cl.172). However, there is room for further improvement in the relationship between the Commissioner and the IPT. If, as argued above, the IPC were to receive public complaints as to the abuse of investigatory powers, they could be more thoroughly investigated because the IPC would have adequate staff.

[332] On January 30, 2014 the Prime Minister told the Select Committee on National Security: 'I do think politicians, police chiefs, the intelligence services have got a role in explaining what this is all about. Snowden inevitably raises questions about "who has access to my data and why"' 'PM: my failure to make case…' *Guardian* January 31, 2014, 8.
[333] e.g. Anderson, 2015, p.303, recommendation 104; RUSI, 2015, 103, 5.30.
[334] cf. Anderson, p.303, recommendation 105.

4.2 The IPT describes itself as 'a judicial body'[335] or a 'court'[336] and it would be best employed as a tribunal in the real sense of the word, that is, as an adversarial forum in which cases brought on behalf of complainants by the IPC (or in which IPC acted as friend of the court) would be heard and 'defended' by the relevant agency. In the nature of things, much of these hearings would need to be held in secret but, wherever possible, they should be held in public and decisions publicised.

Peter Gill

9 December 2015

[335] www.ipt-uk.com/docs/IPTAnnualReportFINAL.pdf p.34, accessed January 3, 2012.
[336] On its web-site: http://www.ipt-uk.com/default.aspx accessed December 4, 2015.

Professor Anthony Glees—written evidence (IPB0150)

1. I come to this subject as someone who has, for many years, worked on intelligence-led security policy and on the broader contextual issues on which such policy touches.

2. In this submission, I would like to offer answers to those of your questions that I feel qualified to answer but preface this with a rider of my own.

3. My position (as a non-technical academic) and as a citizen of the UK who believes in representative liberal democracy and wishes government to deliver security to all its citizens in order that they may benefit from the liberties our political system promotes, I am strongly in favour of the principle and concept of lawful data interception and analysis, indeed think there should be more of it, not less.

4. This applies as much to the combating of serious organised crime of various kinds, including sex criminality, as well as the right against violent extremism and terrorism.

5. I realise that in the aftermath of the Snowden revelations, all democratic governments are obliged to be more open about their use of secret means to deliver security. Unless our intelligence and security community enjoys the trust of citizens as a whole, it cannot fulfil its duties in the context of liberal democracy.

6. That said, I regretted that in his Report, David Anderson QC described RIPA 2000 ('intolerable, unnecessary and undemocratic'). Whilst I think it is clear that he meant by this that this law lacked transparency and was too complex for ordinary citizens to understand, I myself have seen no convincing evidence to indicate that the law itself was any of those things although it is never bad to overhaul and re-package legislation. It is a moot point

7. As I have said in my written (3 February 2014) and subsequent oral evidence to the ISC (14 October 2014), the sine qua non of intrusive intelligence collection is lawfulness, grounded not just in lawful interception and analysis but in the strict adherence to the ECHR.

8. This is something I believe our lawmakers needs to take very seriously the current Bill, if it became law, would become law even if Britain were to reject the ECHR. Unless the safeguards provided by the ECHR were written into any new legislation, I think there would be a grave deficit in the Bill.

9. Equally, those making this law will be making a law that is framed in the context of Britain continuing to be a liberal parliamentary representative democracy.

10. It is perfectly reasonable to argue that if Britain were not a liberal democracy, ‘security’ would have a different meaning and that laws governing the delivery of security should never be capable of abuse by any future, non-democratic regime.

11. In 2014 I felt that it was unnecessary to reflect on this issue in any depth because were Britain to cease to be a liberal democracy, our present security and intelligence community,

and the laws under which they operate, would be abolished. For now, it was sufficient that new laws on security and secret activity should meet the stipulation of the 1989 and 1994 Acts that there should be a statutory duty imposed on our secret agencies to uphold our national liberty.

12. There were no signs in 2014 that Britain would cease to be a liberal parliamentary representative democracy.

13. Today, in 2016, I would now argue that the political landscape seems far less predictable. Whilst one would hope that it remains wholly implausible to think that an extreme British or English government would be formed in the UK, it is no longer unthinkable that those who hold extreme views, whether on the left or the right of our national political life, might achieve ministerial office, perhaps in a coalition with stronger and more traditional parties, and therefore seek to use the extensive powers that the Bill gives our security community for purposes other than those we might intend today.

14. I do not think we should be sleepwalking into 'Stasiland' any more than I believe terrorists and serious organised criminals should be able to exploit the liberties enjoyed by ordinary citizens for their own evil and destructive purposes.

15. Those who like me believe that strong security policy measures are not incompatible with liberal democracy but may, when times are critical, be needed to sustain it, would not wish those measures to be capable of being abused by a future government, whose makeup cannot today be accurately foreseen.

16. I should add that I do not favour changing the current system of authorisation but could accept the concept of the 'double lock' were it necessary to get the Bill made law.

17. I believe the authorisation of warrants in the pursuit of national security concerns is an appropriate task for a very senior politician to execute (i.e. the Home Secretary). I do not believe that the work involved is either too onerous or inappropriate for any Home Secretary to carry out. I certainly do not believe that the responsibility for approving warrants should be given simply to a judicial panel. This is partly because we do not elect judges in this country, nor should we necessarily, partly because if a wrong decision is made, a judge, or judges, cannot easily be held to account for errors and partly because it would be foolish to regard the judiciary as being simply apolitical and objective when it comes to national security.

Turning to the specific questions you ask:

Overarching/thematic questions: Are the powers sought necessary?

- Has the case been made, both for the new powers and for the restated and clarified existing powers?
- Are the powers sought legal? YES
- Are the powers compatible with the Human Rights Act and the ECHR? Is the requirement that they be exercised only when necessary and proportionate fully addressed? YES Are they sufficiently clear and accessible on the face of the draft

Bill? YES Is the legal framework such that CSPs (especially those based abroad) will be persuaded to comply? YES

Are concerns around accessing journalists', legally privileged and MPs' communications sufficiently addressed? NO

- Are the powers sought workable and carefully defined? YES

- Are the technological definitions accurate and meaningful (e.g. content vs communications data, internet connection records etc.)? Does the draft Bill adequately explain the types of activity that could be undertaken under these powers? Is the wording of the powers sustainable in the light of rapidly evolving technologies and user behaviours? Overall is the Bill future-proofed as it stands?

NOT COMPETENT TO ANSWER THESE QUESTIONS

- Are the powers sought sufficiently supervised? YES
- Is the authorisation process appropriate? YES Will the oversight bodies be able adequately to scrutinise their operation? YES What ability will Parliament and the public have to check and raise concerns about the use of these powers? SUFFICIENT

Specific questions: General

- To what extent is it necessary for (a) the security and intelligence services and (b) law enforcement to have access to investigatory powers such as those contained in the Draft Investigatory Powers Bill? I DON'T UNDERSTAND THIS QUESTION

- Are there any additional investigatory powers that security and intelligence services or law enforcement agencies should have which are not included in the draft Bill? NOT COMPETENT TO ANSWER
- Are the new offences proposed in the draft Bill necessary? YES Are the suggested punishments appropriate? YES

Interception

- Are there sufficient operational justifications for undertaking (a) targeted and (b) bulk interception? YES ON BOTH COUNTS
- Are the proposed authorisation processes for such interception activities appropriate? YES BUT I AM PREFER POLITICAL RATHER THAN JUDICIAL CONTROL OVER THE DECISION Is the proposed process for authorising urgent warrants workable? YES
- Are the proposed safeguards sufficient for the secure retention of material obtained from interception? YES
- How well does the current process under Mutual Legal Assistance Treaties (MLATs) work for the acquisition of communications data? NOT COMPETENT TO ANSWER What will be the effect of the extra-territorial application of the provisions on communications data in the draft Bill?

NOT COMPETENT TO ANSWER

Communications Data

- Are the definitions of content and communications data (including the distinction between 'entities' and 'events') sufficiently clear and practical for the purposes of accessing such data?

YES

- Does the draft Bill allow the appropriate organisations, and people within those organisations, access to communications data?

YES

- Are there sufficient operational justifications for accessing communications data in bulk? YES· Is the authorisation process for accessing communications data appropriate?

YES

Data Retention

- Do the proposed authorisation regime and safeguards for bulk data retention meet the requirements set out in the CJEU Digital Rights Ireland and the Court of Appeal Davis judgments?

NOT COMPETENT TO ANSWER THIS

- Is accessing Internet Connection Records essential for the purposes of IP resolution and identifying of persons of interest? YES ABSOLUTELY Are there alternative mechanisms? NO Are the proposed safeguards on accessing Internet Connection Records data appropriate? YES
- Are the requirements placed on service providers necessary and feasible? YES

Equipment Interference

- Should the security and intelligence services have access to powers to undertake (a) targeted and (b) bulk equipment interference? YES ON BOTH COUNTS Should law enforcement also have access to such powers? YES
- Are the authorisation processes for such equipment interference activities appropriate? YES
- Are the safeguards for such activities sufficient? YES

Bulk Personal Data

- Is the use of bulk personal datasets by the security and intelligence services appropriate? YES Are the safeguards sufficient for the retention and access of potentially highly sensitive data? YES

Oversight

- What are the advantages and disadvantages of the proposed creation of a single Judicial Commission to oversee the use of investigatory powers? SEE ABOVE; THERE ARE SERIOUS POLITICAL DISADVANTAGES TO ANY OVER-INVOLVEMENT OF UNELECTED JUDGES

- Would the proposed Judicial Commission have sufficient powers, resources and independence to perform its role satisfactorily? I DO NOT BELIEVE SO

- Are the appointment and accountability arrangements for Judicial Commissioners appropriate? I HAVE NO EXPERT KNOWLEDGE BUT I WOULD DOUBT THIS

- Are the new arrangements for the Investigatory Powers Tribunal including the possibility of appeal adequate or are further changes necessary? YES

Professor Anthony Glees MA M Phil D Phil (Oxon)

January 2015

Global Network Initiative (GNI)—written evidence (IPB0080)

1. The Global Network Initiative (GNI) welcomes the opportunity to provide this written submission to the Joint Committee on the Draft Investigatory Powers Bill. We have chosen to focus our submission on five specific issues, all of which relate to the United Kingdom's commitment to establish a world-leading legal framework and its important role as a standard setter for human rights and the rule of law around the globe:

    (I) Provisions on extra-territorial requests for user data
    (II) The need for a responsible and sustainable legal framework for international data
    (III) Authorisation of bulk collection of communications and communications-related data
    (IV) Provisions that would weaken encryption technologies
    (V) Absence of adequate mechanisms for transparency and accountability for surveillance powers

2. The GNI is a multi-stakeholder group of companies, civil society organisations (including human rights and press freedom groups), investors and academics, who have created a collaborative approach to protect and advance freedom of expression and privacy in the information communications and technology (ICT) sector. Formed in 2008, GNI has developed a set of Principles and Implementation Guidelines to guide responsible company action when facing requests from governments around the world that could impact the freedom of expression and privacy rights of users. These Principles and Implementation Guidelines are based on international human rights standards and are attached to this written evidence in Appendix A. Appendix B has a full list of participants and observers of GNI.

(I) Provisions on extra-territorial requests for user data

3. The GNI has previously expressed concern at provisions contained in the proposed Communications Data Bill of 2012 and the Data Retention and Investigatory Powers Act of 2014 which required communications service providers to respond to requests for user data relating to services operated outside of the U.K. government's jurisdiction.[337] The GNI notes that the Draft Investigatory Powers Bill would replicate and expand on these requirements by asserting jurisdiction over such services for seven out of the eight major powers contained in the Bill.[338]

4. By asserting extraterritorial jurisdiction, the draft Bill could provide unintended

[337] Global Network Initiative, 'Written Evidence to the Communications Data Bill Joint Scrutiny Committee', 23 August 2012, available at http://www.globalnetworkinitiative.org/sites/default/files/GNI%20submission%20on%20U.K.%20comms%20data%20bill%2023%20August%202012.pdf; Open Letter to Prime Minister David Cameron regarding the Data Retention and Investigatory Powers Bill, 14 July 2014, available at http://www.globalnetworkinitiative.org/sites/default/files/GNI%20Open%20Letter%20to%20U.K.%20Prime%20Minister%20-%20July%202014.pdf.

[338] See, e.g., sections 31, 69 (referring to communications data), 79 (referring to data retention), 100 (referring to equipment interference), 108 (referring to bulk interception), 116(3), 130(3) (referring to bulk acquisition), and 145(3).

justification for similar actions by other governments, including those that seek to limit freedom of expression and other human rights online. We are concerned that the effect of passing this legislation will be to encourage other governments to expand claims of jurisdiction without regard to the law applicable to the service. We urge the Committee to be mindful of these consequences, including the risk of retaliatory action by other governments on the privacy rights of U.K. citizens at home and abroad, when considering this legislation. Extra-territorial assertions of jurisdiction create a conflict of laws situation and further complicate the international legal framework at a time when the goal for all stakeholders (users, government agencies and companies) is greater transparency and clearer accountability. This situation would increase uncertainty for all stakeholders and for the rights of U.K. and global citizens.

(II) The need for a responsible and sustainable legal framework for international data

5. The rise of global cloud computing, electronic payment platforms and social media, as well as a global security threat, makes urgent the creation of a responsible and sustainable international framework of laws for data. Independent reviews of the United Kingdom's investigatory and law enforcement data sharing powers performed by David Anderson QC, Sir Nigel Sheinwald, and the Royal United Services Institute delivered a broad consensus that the draft Bill must operate as part of a coherent international legal framework, which creates certainty for all stakeholders, clear laws on the acquisition of data, and sustainable solutions for the critical issues of jurisdiction and applicable law. The review performed by Sir Sheinwald in particular recommended that the U.K. government make a concentrated effort to reform existing mutual legal assistance treaties (MLATs) and, where necessary, to develop new bilateral agreements for data. MLAT reform provides the best route to a sustainable and coherent legal framework, rather than the unilateral assertion of limitless jurisdiction as set out in the draft Bill.

6. The existing MLAT arrangements were designed as a mechanism for law enforcement to lawfully obtain data from other jurisdictions. They were negotiated by and between governments, with processes defined in a pre-Internet era. There has been limited modernisation in the intervening years and these processes, and the resources that support them, are today managing significantly higher demand and are under stress. GNI is particularly concerned that without significant reform to the MLAT system, governments around the world will increasingly act unilaterally through measures such as forced data localisation, government mandates that companies provide back doors into hardware or software, or demands that companies take steps that would compromise the security of users' communications.

7. We also note that strong independent judicial oversight is a crucial component in the international cooperation that will be needed to build a new international approach to data amongst democracies with a high respect for the rule of law.

8. GNI recently commissioned a report on reform options and the importance of ongoing

political and financial investment in these critical law enforcement tools.[339] We are engaged in an ongoing dialogue with global companies, government agencies and other stakeholders to encourage the development of a transparent and efficient approach to cross-border law enforcement requests that includes robust protections for free expression and privacy.

9. The GNI is pleased to see that the draft Bill includes provisions to enable reformed MLATs and new international mutual assistance agreements. However, as noted above, we are concerned that the broad extraterritorial powers contained in the Bill and the likely consequences of the adoption of this approach by other governments may ultimately undermine the U.K. government's ability to conclude such agreements. We would invite the Committee to consider carefully the broader ramifications of enshrining such broadly framed and unilateral extraterritorial powers.

(III) Authorisation of bulk collection of communications and communications-related data

10. The GNI notes with disappointment that the draft Bill authorises U.K. government authorities to obtain warrants for the bulk interception of communications sent or received by persons outside the British Islands (sections 106 *et seq*.) and for the collection of communications data (sections 122 *et seq*.). As the GNI has previously expressed, bulk collection of communications data—both content and metadata—threatens privacy and freedom of expression rights and undermines trust in the security of electronic communications services provided by companies. This practice is incompatible with the principles of necessity and proportionality that the legal frameworks for communications surveillance must meet to ensure they are consistent with human rights standards. Rather than engaging in bulk collection, government surveillance programs should be particularised and based on individual suspicion, with independent judicial oversight that is adequately informed.

11. Furthermore, communications surveillance programs that involve bulk collection and are premised on distinguishing nationals from foreigners for increased privacy protections are unlikely to be effective. Both the UN Human Rights Committee and the Office of the UN High Commissioner for Human Rights have emphasised that any interference with the right to privacy must "comp[ly] with the principles of legality, proportionality and necessity regardless of the nationality or location of individuals whose communications are under direct surveillance."[340]

(IV) Provisions that would weaken encryption technologies

12. The GNI is concerned that section 189(4)(c) of the Draft Investigatory Powers Bill creates broad powers for government authorities to undermine the use of encryption technologies. GNI members have contributed evidence to the Joint Scrutiny Committee on the importance of encryption for protecting the private communications and data of

[339] Andrew K. Woods, *Data Beyond Borders: Mutual Legal Assistance in the Internet Age*, The Global Network Initiative (2015), available at: https://globalnetworkinitiative.org/sites/default/files/GNI%20MLAT%20Report.pdf.
[340] Human Rights Committee, Concluding observations on the fourth report of the United States of America, CCPR /C/USA/CO/4 (2014), para. 22; 'The right to privacy in the digital age', Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37 (2014) para. 36.

individuals and organisations. Advances in digital encryption have significantly improved security for individuals online, especially in financial transactions and communications. Encryption technologies are also important around the world for journalists, human rights defenders, persecuted minorities and people's representatives in parliaments and legislatures to be able to communicate confidentially.

13. A global digital economy will depend on user trust: trust that privacy and free expression rights are being protected, and trust that transactions and data are secure. Cybersecurity and network integrity are the foundations of this trust. The GNI recognises that all governments have a responsibility to protect national security and public safety. This important duty will increasingly involve improving the security of computers and networks, protecting citizens from cybercrime, and protecting children online. Government mandates that subvert or weaken digital security make individual users less safe, shrink the space for free expression and privacy and could slow the development and adoption of secure communications technologies. Deliberate undermining of security and encryption technologies also conflicts with legal requirements that companies and governments protect data from intrusion.[341]

(V) Absence of adequate mechanisms for transparency and accountability

14. As a member of the Freedom Online Coalition, the United Kingdom has made a commitment to promote "transparency and independent, effective domestic oversight related to electronic surveillance."[342] The GNI notes that the Draft Investigatory Powers Bill responds to recommendations that the United Kingdom make public a single law authorizing the surveillance of communications. At the same time, the Bill in its current form misses the opportunity to fulfill the state's commitment to greater transparency and accountability regarding its surveillance practices.

15. The GNI has recommended that governments disclose information about the surveillance demands they make on companies, including the number of surveillance demands, the number of user accounts affected by those demands, the specific legal authority for each of those demands, and whether the demand sought communications content or non-content or both. Companies should also be permitted to disclose the number of demands that they receive, how they respond to them, and the technical requirements for surveillance that they are legally bound to install, implement, and comply with. In addition to purely statistical data, governments should also make publicly available the laws and legal interpretations authorizing electronic surveillance, including executive orders, legal opinions that are relied on by executive officials, and court orders. GNI recommends that governments disclose to the victim that unlawful surveillance has taken place as soon as practical, as well as make public disclosures

[341] See, e.g., **Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Article 4; Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Article 17; see also, Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, 2013/0027 (COD).**

[342] Recommendations for Freedom Online, adopted in Tallinn, Estonia, on April 28, 2014 by Ministers of the Freedom Online Coalition ('Tallinn Agenda').

regarding the scope of unlawful surveillance and remedial and disciplinary actions taken.[343] This is consistent with the recommendations of Sir Nigel Sheinwald, who called on the U.K. government to "look at how it can improve transparency around the number and nature of our requests to domestic and overseas Communication Service Providers."[344]

16. Although sections 171 *et seq*. of the Bill contain some of the aforementioned safeguards, the GNI considers that mechanisms for transparency and public accountability regarding the conduct of communications surveillance are generally weak. Section 66(2) provides communications service providers with a "reasonable excuse" to disclose data requests to users, but this does not occur by default, and it remains an offence to disclose a warrant under other powers. We would urge the Committee to consider how users can have meaningful redress under the new oversight regime without transparency about authorised intrusions into their privacy.

Conclusion

17. The United Kingdom's policy debate leading up to the drafting of the current Investigatory Powers Bill has been watched closely by government and non-government actors around the world. The aforementioned reviews of David Anderson QC, Sir Nigel Sheinwald, and the Royal United Services Institute have set a high standard for public discussion, concurring that these government powers should be clearly set out in a single statute, should be transparent to users, and should raise standards for democratic and judicial oversight and provide a model for other jurisdictions. GNI welcomes changes to the Bill that meet these important recommendations.

18. We continue, however, to have serious concerns about the unilateral extra-territorial reach of laws outside of international legal structures and the precedent this sets for other governments. We remain very concerned about the provisions for bulk interception and collection of communications data, the level of transparency and accountability that the Bill sets for surveillance powers, and the impact on individuals if security and encryption standards are weakened. We are hopeful that this scrutiny process will highlight urgency for the United Kingdom to help create and encourage a responsible and sustainable global framework for global data for the long term. This framework should rely on the rule of law and uphold international standards for free expression and privacy.

19. The GNI is grateful for the opportunity to contribute to the important work of the Joint Committee. Our staff and membership are available to members to answer questions on our submission, and we will continue to offer a constructive and cross-sector

[343] Global Network Initiative, 'Getting Specific about Transparency, Privacy, and Free Expression Online', November 5, 2014, available at: http://www.globalnetworkinitiative.org/news/getting-specific-about-transparency-privacy-and-free-expression-online.

[344] Summary of the Work of the Prime Minister's Special Envoy on Intelligence and Law Enforcement Data Sharing, Sir Nigel Sheinwald, available at: https://www.gov.U.K./government/uploads/system/uploads/attachment_data/file/438326/Special_Envoy_work_summary_final_for_CO_website.pdf.

collaborative forum for developing solutions that advance privacy and freedom of expression around the world.

Appendix A
The Global Network Initiative Principles
Preamble

These Principles on Freedom of Expression and Privacy ("the Principles") have been developed by companies, investors, civil society organizations and academics (collectively "the participants").

These Principles are based on internationally recognized laws and standards for human rights, including the Universal Declaration of Human Rights ("UDHR"), the International Covenant on Civil and Political Rights ("ICCPR") and the International Covenant on Economic, Social and Cultural Rights ("ICESCR").[1,2]

All human rights are indivisible, interdependent, and interrelated: the improvement of one right facilitates advancement of the others; the deprivation of one right adversely affects others. Freedom of expression and privacy are an explicit part of this international framework of human rights and are enabling rights that facilitate the meaningful realization of other human rights.[3]

The duty of governments to respect, protect, promote and fulfill human rights is the foundation of this human rights framework. That duty includes ensuring that national laws, regulations and policies are consistent with international human rights laws and standards on freedom of expression and privacy.

Information and Communications Technology (ICT) companies have the responsibility to respect and protect the freedom of expression and privacy rights of their users. ICT has the potential to enable the exchange of ideas and access to information in a way that supports economic opportunity, advances knowledge and improves quality of life.

The collaboration between the ICT industry, investors, civil society organizations, academics and other stakeholders can strengthen efforts to work with governments to advance freedom of expression and privacy globally.

For these reasons, these Principles and their accompanying Implementation Guidelines establish a framework to provide direction and guidance to the ICT industry and its stakeholders in protecting and advancing the enjoyment of human rights globally.

The participants have also developed a multi-stakeholder governance structure to ensure accountability for the implementation of these Principles and their continued relevance, effectiveness and impact. This structure incorporates transparency with the public, independent assessment and multi-stakeholder collaboration.

The participants will seek to extend the number of organizations from around the world supporting these Principles so that they can take root as a global standard.

Freedom of Expression

Freedom of opinion and expression is a human right and guarantor of human dignity. The right to freedom of opinion and expression includes the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

Freedom of opinion and expression supports an informed citizenry and is vital to ensuring public and private sector accountability. Broad public access to information and the freedom to create and communicate ideas are critical to the advancement of knowledge, economic opportunity and human potential.

The right to freedom of expression should not be restricted by governments, except in narrowly defined circumstances based on internationally recognized laws or standards.[5] These restrictions should be consistent with international human rights laws and standards, the rule of law and be necessary and proportionate for the relevant purpose.[6, 7]

Participating companies will respect and protect the freedom of expression of their users by seeking to avoid or minimize the impact of government restrictions on freedom of expression, including restrictions on the information available to users and the opportunities for users to create and communicate ideas and information, regardless of frontiers or media of communication.

Participating companies will respect and protect the freedom of expression rights of their users when confronted with government[8] demands, laws and regulations to suppress freedom of expression, remove content or otherwise limit access to information and ideas in a manner inconsistent with internationally recognized laws and standards.

Privacy

Privacy is a human right and guarantor of human dignity. Privacy is important to maintaining personal security, protecting identity and promoting freedom of expression in the digital age.

Everyone should be free from illegal or arbitrary interference with the right to privacy and should have the right to the protection of the law against such interference or attacks.[9]

The right to privacy should not be restricted by governments, except in narrowly defined circumstances based on internationally recognized laws and standards. These restrictions should be consistent with international human rights laws and standards,

the rule of law and be necessary and proportionate for the relevant purpose.

Participating companies will employ protections with respect to personal information in all countries where they operate in order to protect the privacy rights of users.

Participating companies will respect and protect the privacy rights of users when confronted with government demands, laws or regulations that compromise privacy in a manner inconsistent with internationally recognized laws and standards.

Responsible Company Decision Making

The implementation of these Principles by participating companies requires their integration into company decision making and culture through responsible policies, procedures and processes.

Participating companies will ensure that the company Board, senior officers and others responsible for key decisions that impact freedom of expression and privacy are fully informed of these Principles and how they may be best advanced.

Participating companies will identify circumstances where freedom of expression and privacy may be jeopardized or advanced and integrate these Principles into their decision making in these circumstances.

Participating companies will implement these Principles wherever they have operational control. When they do not have operational control, participating companies will use best efforts to ensure that business partners, investments, suppliers, distributors and other relevant related parties follow these Principles.[10, 11, 12]

Multi-stakeholder Collaboration

The development of collaborative strategies involving business, industry associations, civil society organizations, investors and academics will be critical to the achievement of these Principles.

While infringement on freedom of expression and privacy are not new concerns, the violation of these rights in the context of the growing use of ICT is new, global, complex and constantly evolving. For this reason, shared learning, public policy engagement and other multi-stakeholder collaboration will advance these Principles and the enjoyment of these rights.

Participants will take a collaborative approach to problem solving and explore new ways in which the collective learning from multiple stakeholders can be used to advance freedom of expression and privacy.

Individually and collectively, participants will engage governments and international institutions to promote the rule of law and the adoption of laws, policies and practices that protect, respect and fulfill freedom of expression and privacy.[13]

Governance, Accountability and Transparency

These Principles require a governance structure that supports their purpose and ensures their long term success.

To ensure the effectiveness of these Principles, participants must be held accountable for their role in the advancement and implementation of these principles.

Participants will adhere to a collectively determined governance structure that defines the roles and responsibilities of participants, ensures accountability and promotes the advancement of these Principles.

Participants will be held accountable through a system of (a) transparency with the public and (b) independent assessment and evaluation of the implementation of these Principles.

Annex A: Definitions

Freedom of Expression: Freedom of expression is defined using Article 19 of the Universal Declaration of Human Rights (UDHR) and Article 19 of the International Covenant on Civil and Political Rights (ICCPR):

UDHR: Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

ICCPR: 1. Everyone shall have the right to hold opinions without interference. 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice. 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals.

Privacy: Privacy is defined using Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR):

UDHR: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

ICCPR: 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.

Rule of Law: A system of transparent, predictable and accessible laws and independent legal institutions and processes which respect, protect, promote and fulfill human rights.

Personal Information: Participants are aware of the range of definitions for "personal information" or "personally identifiable information" and acknowledge that these definitions vary between jurisdictions. These Principles use the term "personal information" and interpret this to mean information that can, alone or in aggregate, be used to identify or locate an individual (such as name, email address or billing information) or information which can be reasonably linked, directly or indirectly, with other information to identify or locate an individual.

User: Any individual using a publicly available electronic communications service, for private or business purposes, with or without having subscribed to this service.

Best Efforts: The participating company will, in good faith, undertake reasonable steps to achieve the best result in the circumstances and carry the process to its logical conclusion.

Annex B: End Notes

[1] It is recognized that other regional human rights instruments address the issues of freedom of expression and privacy, including: The European Convention, implemented by the European Court of Human Rights; the American Convention, implemented by the Inter-American Court of Human Rights and Inter-American Commission; and the Organization of African Unity, implemented by the African Commission on Human and People's Rights.

[2] These Principles have also been drafted with reference to the World Summit on the Information Society Tunis Agenda for the Information Society.

[3] It should be noted that the specific scope of these Principles is limited to freedom of expression and privacy.

[4] Taken from Article 19 of Universal Declaration of Human Rights and Article of 19 of the International Covenant on Civil and Political Rights. It should be noted that these Articles reference the right to "freedom of opinion and expression", and then describe the limited circumstances in which the right to "freedom of expression" (i.e. not opinion) can be restricted. That is the approach taken by these Principles.

[5] The narrowly defined circumstances should be taken from Article 19 of the International Covenant on Civil and Political Rights (ICCPR), namely the actions necessary to preserve national security and public order, protect public health or morals, or safeguard the rights or reputations of others. The scope of permissible restrictions provided in Article 19(3) of the ICCPR is read within the context of further interpretations issued by international human rights bodies, including the Human Rights Committee and the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.

[6] See Annex A for an illustrative definition of Rule of Law.

[7] These Principles have been drafted with reference to the Johannesburg Principles on National Security, Freedom of Expression and Access to Information. The Johannesburg Principles provide further guidance on how and when restrictions to freedom of expression may be exercised.

[8] Participating companies will also need to address situations where governments may make demands through proxies and other third parties.

[9] Taken from Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights.

[10] "Operational control" means the power, directly or indirectly, to direct or cause the direction of the management and policies of the entity. This may be by contract, ownership of voting stock or representation on the Board of Directors or similar governing body.

[11] See Annex A for a definition of Best Efforts.

[12] It is recognized that the influence of the participating company will vary across different relationships and contractual arrangements. It is also recognized that this principle applies to business partners, suppliers, investments, distributors and other relevant related parties that are involved in the participating company's business in a manner that materially affects the company's role in respecting and protecting privacy and freedom of expression. The participating company should prioritize circumstances where it has greatest influence and/or where the risk to freedom of expression and privacy is at its greatest.

[13] It is recognized that participants may take different positions on specific public policy proposals or strategies, so long as they are consistent with these Principles.

The Global Network Initiative Implementation Guidelines

Purpose of This Document

The Principles on Freedom of Expression and Privacy (the "Principles") have been created to provide direction and guidance to the Information and Communications Technology ("ICT") industry and its stakeholders in protecting and advancing the

enjoyment of these human rights globally.

These Implementation Guidelines provide further details on how participating companies will put the Principles into practice. The purpose of this document is to:

- Describe a set of actions which constitute compliance with the Principles.
- Provide companies with guidance on how to implement the Principles.
- As described in the accompanying Governance, Accountability and Learning Framework, each participating company will be assessed on their progress implementing the Principles after two years and annually thereafter.

The effectiveness of these Implementation Guidelines will be reviewed and assessed as experience in implementation of the Principles grows. The review process will include:

- Removing, revising or adding guidelines as appropriate.
- Considering the development of different versions of the Implementation Guidelines that may be tailored to specific regions or sectors.

Responsible Company Decision Making

Board Review, Oversight and Leadership

The Boards of participating companies will incorporate the impact of company operations on freedom of expression and privacy into the Board's review of the business.

The Board will:

- Receive and evaluate regular reports from management on how the commitments laid out in the Principles are being implemented.
- Review freedom of expression and privacy risk within the overall risk management review process.
- Participate in freedom of expression and privacy risk training as part of overall Board education.

Application Guidance: *"Board" could mean a Management Board or Executive Board if these are more appropriate for the participating company's structure.*

Human Rights Impact Assessments

Participating companies will employ human rights impact assessments to identify circumstances when freedom of expression and privacy may be jeopardized or advanced, and develop appropriate risk mitigation strategies when:

- Reviewing and revising internal procedures for responding to government demands for user data or content restrictions in existing markets
- Entering new markets, particularly those where freedom of expression and privacy are not well protected.

- Reviewing the policies, procedures and activities of potential partners, investments, suppliers and other relevant related parties for protecting freedom of expression and privacy as part of its corporate due diligence process.
- Designing and introducing new technologies, products and services.

The human rights impact assessments will be undertaken to different levels of detail and scope depending on the purpose of the impact assessment. However, participating companies should:

- Prioritize the use of human rights impact assessments for markets, products, technologies and services that present the greatest risk to freedom of expression and privacy or where the potential to advance human rights is at its greatest.
- Update human rights impact assessments over time, such as when there are material changes to laws, regulations, markets, products, technologies, or services.
- Draw upon resources from human rights groups, government bodies, international organizations and materials developed as part of this multi-stakeholder process.
- Include a consideration of relevant local laws in each market and whether the domestic legal systems conform to rule of law requirements.
- Utilize learning from real life cases and precedents.
- Focus on potential partners, investments, suppliers and other relevant related parties that are involved in the participating company's business in a manner that materially affects the company's role in respecting and protecting privacy and freedom of expression.
- Incorporate the outputs of human rights impact assessments into other company processes, such as corporate risk assessments and due diligence.

Partners, Suppliers and Distributors
Participating companies will follow these Principles and Implementation Guidelines in all circumstances when they have operational control.

When the participating company does not have operational control it will use best efforts to ensure that business partners, investments, suppliers, distributors and other relevant related parties follow the Principles.

Participating companies should focus their efforts on business partners, investments, suppliers, distributors and other relevant related parties that are involved in the participating company's business in a manner that materially affects the company's role in respecting and protecting freedom of expression and privacy. The participating company should prioritize circumstances where it has the greatest influence and/or where the risk to freedom of expression and privacy is at its greatest.

Application Guidance: *It is assumed that this approach will be taken in all relevant*

contracts signed after committing to the Principles and to all relevant pre-existing contracts.

Application Guidance: *"Operational control" means the power, directly or indirectly, to direct or cause the direction of the management and policies of the entity. This may be by contract, ownership of voting stock or representation on the Board of Directors or similar governing body.*

Application Guidance: *It is recognized that the influence of participating companies will vary across different relationships and contractual arrangements. See the definition of "best efforts" provided in Annex A.*

Integration into Business Operations
Participating companies will develop appropriate internal structures and take steps throughout their business operations to ensure that the commitments laid out in the Principles are incorporated into company analysis, decision making and operations.

Over time this will include:

Structure
The creation of a senior-directed human rights team, including the active participation of senior management, to design, coordinate and lead the implementation of the Principles.

Application Guidance: *This team may build on existing internal corporate structures, such as corporate social responsibility, policy, privacy or business ethics teams.*

Ensuring that the procedures related to government demands implicating users' freedom of expression or privacy rights are overseen and signed-off by an appropriate and sufficiently senior member of the company's management and are appropriately documented.

Procedures
Establishing written procedures that ensure consistent implementation of policies that protect freedom of expression and privacy and documenting compliance with these policies. Documentation of policies and compliance should be sufficiently detailed as to enable later internal and external review.

Establishing a means of remediation when business practices that are inconsistent with the Principles are identified, including meaningful steps to ensure that such inconsistencies do not recur.

Incorporating freedom of expression and privacy compliance into assurance processes to ensure compliance with the procedures laid out in the Principles.

Maintaining a record of requests and demands for government restrictions to freedom of expression and access to personal information.

Employees
Communicating the Principles to all employees, such as through the company intranet, and integrating the company's commitment to the Principles through employee training or orientation programs.

Providing more detailed training for those corporate employees who are most likely to face freedom of expression and privacy challenges, based on human rights impact assessments. This may include staff in audit, compliance, legal, marketing, sales and business development areas. Where appropriate and feasible, the orientation and training programs should also be provided to employees of relevant related parties such as partners, suppliers and distributors.

Complaints and Assistance
Developing escalation procedures for employees seeking guidance in implementing the Principles.

Providing whistle-blowing mechanisms or other secure channels through which employees and other stakeholders can confidentially or anonymously report violations of the Principles without fear of associated punishment or retribution.

Application Guidance: *For example, each company might appoint or designate an internal ombudsman or auditor to monitor the company's business practices relating to freedom of expression and privacy.*

Freedom of Expression

Government Demands, Laws and Regulations
Participating companies will encourage governments to be specific, transparent and consistent in the demands, laws and regulations ("government restrictions") that are issued to restrict freedom of expression online.

Participants will also encourage government demands that are consistent with international laws and standards on freedom of expression. This includes engaging proactively with governments to reach a shared understanding of how government restrictions can be applied in a manner consistent with the Principles.

When required to restrict communications or remove content, participating companies will:

- Require that governments follow established domestic legal processes when they are seeking to restrict freedom of expression.
- Interpret government restrictions and demands so as to minimize the negative effect on freedom of expression.

- Interpret the governmental authority's jurisdiction so as to minimize the negative effect on to freedom of expression.

Application Guidance: *It is recognized that the nature of jurisdiction on the internet is a highly complex question that will be subject to shifting legal definitions and interpretations over time.*

- Seek clarification or modification from authorized officials when government restrictions appear overbroad, not required by domestic law or appear inconsistent with international human rights laws and standards on freedom of expression.

Application Guidance: *Overbroad could mean, for example, where more information is restricted than would be reasonably expected based on the asserted purpose of the request.*

- Request clear written communications from the government that explain the legal basis for government restrictions to freedom of expression, including the name of the requesting government entity and the name, title and signature of the authorized official.

Application Guidance: *Written demands are preferable, although it is recognized that there are certain circumstances, such as where the law permits verbal demands and in emergency situations, when communications will be oral rather than written.*

- Adopt policies and procedures to address how the company will respond in instances when governments fail to provide a written directive or adhere to domestic legal procedure. These policies and procedures shall include a consideration of when to challenge such government demands.
- Challenge the government in domestic courts or seek the assistance of relevant government authorities, international human rights bodies or non-governmental organizations when faced with a government restriction that appears inconsistent with domestic law or procedures or international human rights laws and standards on freedom of expression

Application Guidance: *It is recognized that it is neither practical nor desirable for participating companies to challenge in all cases. Rather, participating companies may select cases based on a range of criteria such as the potential beneficial impact on freedom of expression, the likelihood of success, the severity of the case, cost, the representativeness of the case and whether the case is part of a larger trend.****Application Guidance:*** *Policies and procedures adopted by participating companies will address situations where governments may make demands through proxies and other third parties to evade domestic legal procedures.*

Communications With Users
Participating companies will seek to operate in a transparent manner when required

by government to remove content or otherwise limit access to information and ideas. To achieve this, participating companies will, unless prohibited by law:

- Clearly disclose to users the generally applicable laws and policies which require the participating company to remove or limit access to content or restrict communications.
- Disclose to users in a clear manner the company's policies and procedures for responding to government demands to remove or limit access to content or restrict communications.
- Give clear, prominent and timely notice to users when access to specific content has been removed or blocked by the participating company or when communications have been limited by the participating company due to government restrictions. Notice should include the reason for the action and state on whose authority the action was taken.

Privacy

Data Collection

Participating companies will assess the human rights risks associated with the collection, storage, and retention of personal information in the jurisdictions where they operate and develop appropriate mitigation strategies to address these risks.

Government Demands, Laws and Regulations

Participating companies will encourage governments to be specific, transparent and consistent in the demands, laws and regulations ("government demands") that are issued regarding privacy online.

Participating companies will also encourage government demands that are consistent with international laws and standards on privacy. This includes engaging proactively with governments to reach a shared understanding of how government demands can be issued and implemented in a manner consistent with the Principles.

Participating companies will adopt policies and procedures which set out how the company will assess and respond to government demands for disclosure of personal information. When required to provide personal information to governmental authorities, participating companies will:

- Narrowly interpret and implement government demands that compromise privacy.
- Seek clarification or modification from authorized officials when government demands appear overbroad, unlawful, not required by applicable law or inconsistent with international human rights laws and standards on privacy.

Application Guidance: *Overbroad could mean, for example, where more personal information is requested than would be reasonably expected based on the asserted purpose of the request.*

- Request clear communications, preferably in writing, that explains the legal basis for government demands for personal information including the name of the requesting government entity and the name, title and signature of the authorized official.

Application Guidance: *Written demands are preferable, although it is recognized that there are certain circumstances, such as where the law permits verbal demands and in emergency situations, when communications will be oral rather than written.*

- Require that governments follow established domestic legal processes when they are seeking access to personal information.
- Adopt policies and procedures to address how the company will respond when government demands do not include a written directive or fail to adhere to established legal procedure. These policies and procedures shall include a consideration of when to challenge such government demands.
- Narrowly interpret the governmental authority's jurisdiction to access personal information, such as limiting compliance to users within that Country.

Application Guidance: *It is recognized that the nature of jurisdiction on the internet is a highly complex question that will be subject to shifting legal definitions and interpretations over time.*

- Challenge the government in domestic courts or seek the assistance of relevant authorities, international human rights bodies or non-governmental organizations when faced with a government demand that appears inconsistent with domestic law or procedures or international human rights laws and standards on privacy.

Application Guidance: *It is recognized that it is neither practical nor desirable for participating companies to challenge in all cases. Rather, participating companies may select cases based on a range of criteria such as the potential beneficial impact on privacy, the likelihood of success, the severity of the case, cost, the representativeness of the case and whether the case is part of a larger trend.*

Application Guidance: *Policies and procedures adopted by participating companies will address situations where governments may make demands through proxies and other third parties to evade domestic legal procedures.*

Communications with Users

Participating companies will seek to operate in a transparent manner when required to provide personal information to governments. To achieve this, participating companies will:

Application Guidance: *Participating companies will work with the Organization to raise awareness among users regarding their choices for protecting the privacy of their personal information and the importance of company data practices in making those choices.*

- Disclose to users in clear language what generally applicable government laws and policies require the participating company to provide personal information to government authorities, unless such disclosure is unlawful.
- Disclose to users in clear language what personal information the participating company collects, and the participating company's policies and procedures for responding to government demands for personal information.
- Assess on an ongoing basis measures to support user transparency, in an effective manner, regarding the company's data collection, storage, and retention practices.

Multi-stakeholder Collaboration

Engagement in Public Policy
Participants will encourage governments and international institutions to adopt policies, practices and actions that are consistent with and advance the Principles.

Individually or collectively participants will:

- Engage government officials to promote rule of law and the reform of laws, policies and practices that infringe on freedom of expression and privacy.

Application Guidance: *Promoting rule of law reform could include rule of law training, capacity building with law-related institutions, taking public policy positions or external education.*

- Engage in discussions with home governments to promote understanding of the Principles and to support their implementation.
- Encourage direct government-to-government contacts to support such understanding and implementation.
- Encourage governments, international organizations and entities to call attention to the worst cases of infringement on the human rights of freedom of expression and privacy.
- Acknowledge and recognize the importance of initiatives that seek to identify, prevent and limit access to illegal online activity such as child exploitation. The Principles and Implementation Guidelines do not seek to alter participants' involvement in such initiatives.
- Participants will refrain from entering into voluntary agreements that require the participants to limit users' freedom of expression or privacy in a manner inconsistent with the Principles. Voluntary agreements entered into prior to committing to the Principles and which meet this criterion should be revoked within three years of committing to the Principles.

Application Guidance: *It is recognized that participants may take different positions on specific public policy proposals or strategies, so long as they are consistent with these principles.*

Internal Advisory Forum
A confidential multi-stakeholder Advisory Forum will provide guidance to participating companies on emerging challenges and opportunities for the advancement of freedom of expression and privacy.

External Multi-stakeholder Learning Forums Participants will promote global dialogue and understanding of the Principles and share learning about their implementation. Participants will engage with a broad range of interested companies, industry associations, advocacy NGOs and other civil society organizations, universities, governments and international institutions.

Participants will create a global learning, collaboration and communication program. This program will identify stakeholders, topics and forums for learning, collaboration and communication activities.

Application Guidance: *This could include, for example, the Internet Governance Forum, the International Telecommunications Union, the UN Global Compact and the UN Special Representative of the Secretary General on human rights and transnational corporations and other business enterprises.*

Part of this learning program will be an annual Multi-stakeholder Learning Forum focusing on the rights to freedom of expression and privacy, the specific scenarios in which these rights are affected and other broader issues related to the implementation of the Principles.

Where participants have activities or operations in the same countries they will seek to collaborate on the development of local dialogues on relevant prominent issues and emerging concerns in those localities.

Participants will develop and share innovative tools, resources, processes and information that support the implementation of the Principles.

Included in the learning program will be a consideration of the role that tools such as encryption, anonymizing technologies, security enhancements and proxy technologies can play in enabling users to manage their media experiences and protect freedom of expression and privacy.

Governance, Accountability & Transparency

Governance
A multi-stakeholder representative Board will oversee this initiative, described in more detail in the accompanying Governance, Accountability and Learning Framework

document.

Reporting on Implementation
There will be three different levels of reporting on the progress being made to implement the Principles, described in more detail in the accompanying Governance, Accountability and Learning Framework document.

Independent Assessment
There will be a system of independent assessment of the implementation of the Principles, described in more detail in the accompanying Governance, Accountability and Learning Framework document.

Annex A: Definitions

Freedom of Expression: Freedom of expression is defined using Article 19 of the Universal Declaration of Human Rights (UDHR) and Article 19 of the International Covenant on Civil and Political Rights (ICCPR):

UDHR: Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

ICCPR:

1. Everyone shall have the right to hold opinions without interference.
2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:
(a) For respect of the rights or reputations of others;
(b) For the protection of national security or of public order (ordre public), or of public health or morals.

Privacy: Privacy is defined using Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR):

UDHR: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

ICCPR:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.

Rule of Law: A system of transparent, predictable and accessible laws and independent legal institutions and processes, which respect, protect, promote and fulfill human rights.

Personal Information: Participants are aware of the range of definitions for "personal information" or "personally identifiable information" and acknowledge that these definitions vary between jurisdictions. These Implementation Guidelines use the term "personal information" and interpret this to mean information that can, alone or in aggregate, be used to identify or locate an individual (such as name, email address or billing information) or information which can be reasonably linked, directly or indirectly, with other information to identify or locate an individual.

User: Any individual using a publicly available electronic communications service, for private or business purposes, with or without having subscribed to this service.

Best Efforts: The participating company will, in good faith, undertake reasonable steps to achieve the best result in the circumstances and carry the process to its logical conclusion.

Appendix B
Participants in the Global Network Initiative

ICT Companies

Facebook
Google
LinkedIn
Microsoft
Procera Networks
Yahoo!

Academics

Berkman Center for Internet and Society, Harvard University
Center for Business and Human Rights, New York University Stern School of Business
Centro de Estudios en Libertad de Expresión, Universidad de Palermo (Argentina)
Deirdre Mulligan, University of California at Berkeley School of Information
Ernest Wilson, Annenberg School for Communication, University of Southern California
George Washington University Law School

Kyung-Sin Park, Korea University Law School
Nexa Center for Internet and Society, Politecnico di Torino (Italy)
Philip N. Howard, University of Washington and Central European University
Rebecca MacKinnon, New America Foundation
Research Center for Information Law, University of St. Gallen (Switzerland)

Civil Society Organizations

Bolo Bhi
Center for Democracy and Technology
Centre for Internet and Society
Committee to Protect Journalists
Human Rights First
Human Rights in China
Human Rights Watch
Index on Censorship
Institute for Reporters' Freedom and Safety
International Media Support
Internews
PEN American Center
World Press Freedom Committee

Investors

Boston Common Asset Management
Calvert Investments
Church of Sweden
Domini Social Investments
EIRIS Conflict Risk Network
F&C Asset Management
Folksam
Trillium Asset Management
Walden Asset Management

21 December 2015

GreenNet Limited—written evidence (IPB0132)

Introduction

1. Thank you for the opportunity to contribute evidence to the Joint Committee's inquiry into the *Draft Investigatory Powers Bill* published by the Home Office in November 2015.
2. This submission includes part of our evidence already published by the Commons Science and Technology Committee, including an internet glossary[345]. The technological considerations have a significant bearing on human rights and the reasons why what is contemplated in the draft is dangerous, neither necessary nor proportionate, and adds little benefit to existing powers.
3. GreenNet is a small not-for-profit organisation founded before commercial public internet service providers; Prof Peter Willetts of City University states that GreenNet was arguably the first ISP in Britain.[346] GreenNet has considerable technical expertise in providing a wide range of internet services to the non-profit sector, as well as actively countering network abuse, and works to support free software and open standards.

Summary

4. It is very difficult for the public, experts or MPs to assess the draft's likely impacts at this stage owing to the lack of technical coherence, and the absence of draft secondary legislation such as codes and the very probable lack of detail in those too if they are published in March. Generally, we do not refer to specific clauses of the draft, owing to the inchoate nature of many of the concepts introduced in its more contentious parts. In our opinion the committee has a difficult job responding to the paper in a meaningful way, despite being able to draw on findings of the previous committee on the *Draft Communications Data Bill* (DCDB) and the Investigatory Powers Review.
5. Recommendation 18 of the Anderson review is that "There should be no question of progressing proposals for the compulsory retention of third party data before such time as a compelling operational case may have been made, there has been full consultation with CSPs and the various legal and technical issues have been fully bottomed out. None of those conditions is currently satisfied." Not enough information has been released about ICRs (third-party data) for discussion to properly begin, let alone "bottom out".
6. We suggest two options are possible:

- a redraft by an independent panel not including the Home Office that omits Parts 4 (equivalent to the DCDB) and 6 and 7 (bulk powers), adds proper judicial oversight and legal transparency, and tightens definitions against the type of abuse we now

[345]http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25510.html

[346]Willetts, Peter, *Non-Governmental Organizations in World Politics: The Construction of Global Governance*, Routledge, 2010. p113.

know exist. This has the advantage that the result stands some chance of passing public and expert scrutiny, and will not necessarily violate human rights conventions, but will require a further stage in committee; or

- a complete freeze on the legislative process until the proponents give a detailed operational case for their proposed powers, and the exact basis for the £247m costs in the (short-term) impact assessment that can then be assessed by independent experts as recommended in the Anderson report. This has the advantage of giving time for the Home Office to decide whether they would like to withdraw anything on their "Christmas list" of new powers, or think they can provide a coherent justification that would pass technical scrutiny.

7. We agree with evidence given to parliamentarians by James Blessing of ISPA, Prof Ross Anderson, Dr Joss Wright, Prof Bill Buchanan and other experts about the complexity and scale of interference with communications implied by the draft, lack of effectiveness against serious crime, disproportionate burdens that might placed on the UK technology industry and a general absence of meaningful definitions in the draft bill. We also concur with the evidence of Adrian Kennard of ISP Andrews & Arnold, who noted a worrying lack of technical understanding by the Home Office, including around modern network protocols and applications, data protection issues, powers to compel generation of "internet connection records" (ICRs, presumably equivalent to "web logs" as used in the DCDB) and lack of any answer about how they might be generated.
8. The stated constraint of the DRIPA sunset clause is really self-imposed. DRIPA is subject to a legal challenge currently referred to the CJEU, which has previously ruled that the EU Data Retention Directive (DRD) of which DRIPA is an extension is incompatible with the European Charter of Fundamental Rights; also in many EU countries the DRD has been struck down as unconstitutional, without obvious harmful effects; and these powers were new to the UK in 2005.

Questions in Call for Evidence

9. *"Has the case been made, both for the new powers and for the restated and clarified existing powers?"* No. Anderson makes the case for targeted surveillance and interception, but no case has been attempted for mass surveillance and the document attempting to justify or even define ICRs is technically incoherent. Further, we do not accept that bulk powers had ever previously been envisaged or granted by Parliament,[347] so the characterisation as restatement and clarification is misleading.
10. "*Are the powers compatible with the Human Rights Act and the ECHR? Is the requirement that they be exercised only when necessary and proportionate fully*

[347]"As the minister who arranged for the 1994 Intelligence Services Act to pass through Parliament, David Davis says that officials never conveyed, even secretly, how they saw the law as authorising the creation of a joined-up secret national database."
http://www.theregister.co.uk/2015/12/16/big_brother_born_ntac_gchq_mi5_mass_surveillance_data_slurping
Similarly the 2015 amendment to the Computer Misuse Act 1990 to legalise hacking was never debated, nor probably understood, by parliamentarians.

addressed?" No and no. Part 4 is incompatible with the ECHR because the powers have no limits, either technically, or in terms of access to stored data requiring judicial oversight, and does not amount to foreseeable law. Parts 6 and 7 are incompatible with the ECHR as they are grossly disproportionate, including blanket suspicionless surveillance and interception that has already been ruled a violation of Article 8.[348]

11. "*Are they sufficiently clear and accessible on the face of the draft Bill?*" No, part 4 is not just opaque (there is no such thing as an "internet connection record") but suggests the Home Office itself is not clear what law enforcement wants.

12. "*Is the legal framework such that CSPs (especially those based abroad) will be persuaded to comply?*" If they also operate in the UK, they may be compelled to comply. If they do not, Five Eyes data sharing arrangements may come into place. In clear cases, Mutual Legal Assistance Treaties can be used.

13. "*Are concerns around accessing journalists', legally privileged and MPs' communications sufficiently addressed?*" No. Codes of Practice merely mention that these classes are "confidential" and should be treated with greater care, but this is not really possible with mass surveillance. The IoCC stated that judicial pre-authorisation (on all the facts) should be required in these cases.

14. "*Are the technological definitions accurate and meaningful (e.g. content vs communications data, internet connection records etc.)? Does the draft Bill adequately explain the types of activity that could be undertaken under these powers? Is the wording of the powers sustainable in the light of rapidly evolving technologies and user behaviours?*" No, no and no. For more details, see our submission to the S&T committee.

15. "*Overall is the Bill future-proofed as it stands?*" We feel clarity, proportionality and necessity are more important than attempts to "future-proof", which have resulted in general and unlimited powers in Part 4. No legislation is conceivable that will enable complete surveillance all the time, particularly in the case of serious crime where targets are being careful.

16. "*Is the authorisation process appropriate? Will the oversight bodies be able adequately to scrutinise their operation?*" No. Fuzzy or ill-defined powers will be extended in practice, much as they were under RIPA (for example, "thematic" s8(1) warrants), and are more open to abuse than well-defined foreseeable ones. We share concerns that judicial oversight in these proposals is only rubber-stamping the process, and not up to international standards. We would also strongly recommend

[348]Questions of proportionality are very difficult (how much intrusion is justified by one life?) and need public debate. Much work is happening on foundations of human rights that agrees that whether naturalistically derived as inhering in human beings or intersubjective, rights are dynamic and not granted by states. Thus the decision whether a course of action is necessary and proportionate involves the human subjects of that decision, and so far as possible citizenry should be not only informed of but involved in what is proposed. This suggests not assuming total secrecy and having new capabilities ordered by a secretary of state on the basis of a summary prepared for her. The paper uses some of the same phrases as in ECHR Article 8.2: "national security", "economic well-being" and "prevention... of crime". However it is far from clear that they have the same meaning as in the ECHR, and Article 8.2 exceptions can themselves be criticised as over-broad. Unmentioned by the draft is the fact that Article 8.2 restricts these exceptions to the right to privacy to those "in accordance with the law and... necessary in a democratic society". See also Martti Koskainen.

that if these powers are used, the actual record of what they are used for and what effects they have becomes public after a period of time, thus enabling both people to know what the intrusion on their privacy has been and also a debate on whether practice is in accordance with human rights. This is the situation in other countries. While the Interception of Communications Commissioner (IoCC) has made welcome progress in publishing statistics, we still have not seen examples and statistics about when surveillance and interception have been strictly necessary, and when merely possibly helpful or routine.

17. "*What ability will Parliament and the public have to check and raise concerns about the use of these powers?*" If they don't know about them or understand them, not much. The IPT would be the only recourse for Parliament or public, and does not produce rulings purely on the law, but on practice.

18. "*To what extent is it necessary for (a) the security and intelligence services and (b) law enforcement to have access to investigatory powers such as those contained in the Draft Investigatory Powers Bill?*" The agencies have used these powers, but we do not know for what purposes. Law enforcement now *wants* similar capabilities, but the Anderson annexes suggest they might be helpful in marginal cases, not actually necessary.

19. "*Are there any additional investigatory powers that security and intelligence services or law enforcement agencies should have which are not included in the draft Bill?*" No. Nearly every conceivable power is covered, except data-sharing with foreign agencies. The agencies went beyond the explicit powers in RIPA, so may well interpret a new law in a similarly lax way.

20. "*Are the new offences proposed in the draft Bill necessary?*" No, and some are unworkable. ISPs are concerned about the gagging order in 190(8).

21. "*Do the proposed authorisation regime and safeguards for bulk data retention meet the requirements set out in the CJEU Digital Rights Ireland and the Court of Appeal Davis judgments?*" No. *Digital Rights Ireland* rules out mandatory data retention, while the "request filter" is merely a front-end to a massive database.

22. "*What are the advantages and disadvantages of the proposed creation of a single Judicial Commission to oversee the use of investigatory powers?*" One advantage is that issues like hacking are less likely to fall between the gaps; the main disadvantage is the high level of secrecy the Commissioner will be induced to work under, and the possibility of the Commission being "captured". The IoCC can only report on affairs and is further limited by the Justice and Security Act, but should assess not just the number of warrants applied for and granted, but the number of people affected by class-based or thematic warrants, and under which grounds. The idea that a "person" under RIPA 8(1) could be any group of people attending a "high profile event" (ISC report s 43) or "a group of individuals... [where] the case for each warrant would be more or less identical" was a surprise. The Intelligence Services Commissioner should also be allowed to disclose detailed statistics of numbers of people affected, and problems caused by lack of consultation with ministers and lack of technical or legal expertise in government (see paragraphs 236ff of the ISC report, and ministerial confusion in ISC testimony over scope of an 8(4) warrant).

Possible ways forward

23. It seems that the technical advice the Home Office has received has been almost entirely from those companies (eg Detica, Huawei) that are providing supporting solutions to gather, store and access communications data, and quotes from the a few mobile carriers. There has been relatively little discussion with the internet industry as a whole; the Joint Committee on the *draft Communications Data Bill* said "*Before re-drafted legislation is introduced there should be a new round of consultation with technical experts, industry, law enforcement bodies, public authorities and civil liberties groups. This consultation should be on the basis of the narrower, more clearly defined set of proposals... CSPs should be given a clear understanding of the exact nature of the gap which the draft Bill aims to address"*. We see no evidence that this has happened.

24. It might be useful focussing on a simple example such as a missing person case and identifying a mobile device used to tweet or post a message – something still a little more complicated than a RIPA request to a telco for a reverse number lookup. Nowhere have we seen it clarified what extra data is planned to be logged as implied by the impact assessment, and how it would help in such a case; nor much evidence that it has been considered.

25. There is a strong idea underlying at least Part 4 of the draft that legislation can be "future-proofed" by describing things at a conceptual level. However, **it should at least be possible to at deduce roughly how such legislation applies to the current technical environment, and at the moment it is not**. Not being able to do so is equivalent to not being able to discuss that law enforcement ever uses techniques like CCTV, photofit or DNA databases yet having to accept that their use of such unknown techniques might be legal.

26. Not only does the legislation not proceed from defined current needs and then try to generalise for future (unknown) technological development, this technical "flexibility" adds to uncertainty over purpose and legal principle. Like the *Draft Communications Data Bill*, this draft enables the executive to compel virtually anyone to spy on anyone else and make it a criminal offence for them to discuss the practice or process in perpetuity. The main safeguard is that compulsion must be decided by the executive to be for reasons of "national security" or prevention or detection of a "serious crime" or "preventing disorder"[349], which are generally defined not by law but by the same executive.

27. Many of the definitions are very similar to RIPA 2000, but the scope is extended since we no longer have a monopoly or oligopoly of providers. A "private telecommunications system" (clause 193(14)) literally includes a phone, while a "telecommunications operator" (c193(10)) controls a telecommunications system, for example, uses a phone. This literally raises the issue of the "right to whisper". Is private communication deemed to be essentially antisocial? Did Bentham's Panopticon (before being rejected by Mill), or *1984*'s "telescreens" even go this far?

[349]Does this include any Public Order Act offence? Or is it limited by case law? Also refers to ""conduct... for a common purpose"

28. Various leaked documents provide convincing evidence that GCHQ has attempted to gain access to, for example, SIM card manufacturer Gemalto and ISP Belgacom, who are in all respects unremarkable service providers, with the effect of breaking the privacy of ordinary people on a very wide scale.

29. Given the way technology is used now, access to endpoint devices gives disproportionate insight into an ordinary person's personal and political life. People share their confidences with a machine in the assumption that it is an inanimate medium of communication with friends, not one that may be actively spying on them.

30. A draft code of practice or statutory order to be enacted under an investigatory powers bill would need to elaborate precise classes of “equipment interference”, perhaps limited numerically, and not only specify that they are used in the last resort, but also state under what conditions they are considered potentially proportionate.

Human rights issues

31. It would be a mistake to think that legal aspects can ever be cleanly separated from technical aspects. As Lawrence Lessig, professor of law at Harvard put it, “Code is Law”. Thus the inability of this inquiry to reliably assess cost and impact of proposals without fully-worked examples is not totally unrelated to our inability as citizens to judge the same proposals' proportionality.

32. We have not seen the ostensible distinction between “mass” and “bulk” clarified. It is presumed that the government denies mass surveillance because coverage is not expected to reach 100%. Whether or not access is limited by code or law, blanket metadata generation and storage on a service (one example of “bulk personal datasets”) constitutes mass surveillance, affecting all users of the service indiscriminately.

33. Human rights courts have repeatedly confirmed that it is not the analysis of data that is the sole threat to privacy, but the mechanical collection and storage of data violates Article 8 (Kennedy v UK, s162; Amman v Switzerland s 69; Rotaru v Romania s43). Also the Halford case showed that all interception requires the subject to know when they might be being spied on.

34. This engages not just Article 8, but also Article 9 (freedom of conscience), Article 10 (freedom of expression), Article 11 (freedom of association) or Article 14 (freedom from discrimination on "religious, political or other opinion”). Given that acts of equipment interference are supposedly not done for their own sake, but in the context of wider projects of using information for some “national security” effect or prevention of harm (or else they could not be justified), all of these are potentially relevant violations.

35. Human rights treaties and conventions generally suggest targeted interception and surveillance can be justified under certain conditions including necessity for a legitimate aim and proportionality. This is spelled out most fully at a high-level in the *International Principles on the Application of Human Rights to Communications*

Surveillance. [350] However, the cases in mind there are more around CSP data retention than mass (or "bulk") application of ultra-intrusive device interference giving access to local data. It needs to be considered whether extreme measures are compatible with such principles at all.

36. Usually decisions on proportionality are made by a court. It is a question of an entirely different order to weigh what intrusions are necessary to keep tabs on a "radical" group, or a competitor to a notionally British corporation – should anything be done to monitor pure "thoughtcrime"? What are the limits to such operations?

37. These proposals may grant powers to law enforcement previously reserved for the secret services, but there we see nothing to prohibit a class warrant from allowing GCHQ (or indeed law enforcement) access to the content of the co-ordinating "request filter" to be used in data mining or fishing expeditions.

38. How would the bill interact with Data Protection obligations? Is the data processor in this case the service provider, and the data controller is the Home Office, since they determine what personal information is to be kept? It seems possible the Home Office has not even considered CD as personal data, although it clearly is. How do data protection principles apply to data that is retained for a fixed period of time regardless of whether it is of any use? Is a completely different standard of data protection to be applied here than to all other personal data, and if so exactly how?

39. The social effect of government interference would suggest that we are already beyond the point at which a decrease in privacy would improve public safety, at least to any significant extent. As is frequently remarked, perpetrators of acts of truly serious crime (mass murder and injury) are almost always already identified (the exception being the lone wolf Anders Breivik, where monitoring fertiliser and weapon deliveries would have been more effective than creating social graphs). Monitoring like that contemplated here is most developed in Iran, and particularly China, and those countries are good exemplars that interference in the internet medium does not significantly inhibit crime such as fraud or corruption, but can be an effective means of social engineering and suppressing dissent. (Ed Snowden is particularly concerned about how surveillance causes censorship to be internalised.)

40. Nowadays most of us leave a massive digital footprint, capable of being analysed in an automated fashion to provide a partial picture of one's life and interests. In Amsterdam from the 1900s onwards, city authorities collected detailed religious demographic data for benign municipal purposes until the Nazis occupied the Netherlands. Government hacking activities and access to "bulk personal datasets" show that unanticipated use of technology has enabled vast expansion of powers from the days when phone tapping required the laborious attachment of crocodile clips and was reserved for the most serious cases.

41. Just because some information is sometimes available and useful in some cases at a particular period of time, it does not mean that it is or should be equally available or even meaningful in all cases. Nor does it mean that such information will always be equally available as technology changes. As former Home Secretary James Callaghan

[350] available at https://en.necessaryandproportionate.org/files/2014/09/03/np-booklet-2014_english_final_print-ready-2-1_copy_0.pdf

noted, it is a given that senior police will always want more power no matter how much they have.

42. It is the manner in which previous lack of clarity and foreseeability in existing legislation violates human rights and legal principle that has forced for example disclosure (or avowal) of the use of Telecommunications Act s94 and publication of the draft Equipment Interference Code and contributed to the striking down of the EU Data Retention Directive (DRD) as a result of the *Digital Rights Ireland* case. The wide undefined powers in this draft would seem to have more severe problems in that respect.

43. Article 8.1 provides greater protection to the privacy of individuals than to non-natural persons, and this should be reflected in an legislation. One major is with the phrase "national security", which is extremely elastic. In the post-War era it referred to use of armed force against British territory, but there is a danger that it has come to include any cause that is politically expedient to avoid embarrassment or keep information away from the general public, such as by Cyril Smith against a paedophile investigation[351]. Notoriously "national security" was initially accepted by a court as a reason to drop a criminal investigation into corruption into BAE and Saudi Arabia, as though sale of weapons to repressive regimes where they are likely to be used for human rights abuses is in the interests of British "national security".[352] It would be a fallacy to infer from the advanced technical capabilities of GCHQ that it is equally competent as an organisation in its decision-making and all its activities are effectively directed towards, say, counter-terrorism.[353] British counter-intelligence failed to catch a single spy during the entire Cold War.[354]

44. Clandestine organisations charged with bugging individuals and organisations have proved reactionary and discriminatory, such as the FBI against the US civil rights movement. In the UK, MI5 targeted the National Union of Mineworkers. In a more recent scandal, it was revealed that the secret police Special Demonstration Squad collaborated with private "blacklisting" interests, and systematically infiltrated groups working for environmental and animal rights for as yet unexplained reasons, planting *agents provocateurs* among anti-climate-change activists.[355] Similarly, police have wasted legal resources to ensure peace activist John Catt, aged 89, is listed on a "National Domestic Extremism Database".

45. As mentioned here, but not in the draft, exceptions from Article 8.1 on privacy should support "a democratic society". This has several implications. Democracy has a number of important prerequisites including free access to untainted information, freedom from coercion and ability to associate with radical viewpoints, not merely an occasional choice between a limited set of establishment political parties. Therefore, firstly, information about how these exceptions are applied must themselves be subject to public scrutiny. That we are only now discussing in inadequate and vague terms, shows this condition has yet to be met. Secondly, use of "national security" exceptions must not undermine the right to free association

[351]eg http://www.lbc.co.uk/when-cyril-smith-forced-journalist-to-drop-paedophile-story-106571
[352]See Cornerhouse resources at http://www.thecornerhouse.org.uk/resources/results/taxonomy%3A90
[353]Adam Curtis, http://www.bbc.co.uk/blogs/adamcurtis/posts/BUGGER (2014)
[354]Christopher Andrew, *The Defence of the Realm: The Authorised History of MI5* (2009)
[355]Paul Lewis and Rob Evans, *Undercover: The True Story of Britain's Secret Police* (2014)

for any peaceful purpose. "National security" must be given defined limits. Its continual redefinition by the executive and the security establishment can only lead to a dangerous concentration of power that will be abused in the interests of the few.

46. The Report of the Interception of Communications Commissioner (IoCC, March 2015, s7.89) strongly recommends pre-authorisation for journalists' sources.[356]

47. There is nothing here describing the sharing of resources obtained by hacking among intelligence partners. Thus it is not clear that operations started by GCHQ are not further exploited by, say, the NSA outside these laws. The FISA Amendment Act allowed US services to spy on non-US citizens purely on the grounds of US political interests.

Concluding remarks

48. The concept of an "Internet Connection Record" is perhaps the most prominent of the problematic areas in the Home Office draft, along with the many other new powers to weaken security and the draconian, impractical and unnecessary new disclosure offences particularly for CSPs in paragraphs 31, 77(2), 101, 133, 148 and 190(8). Questions of the feasibility and proportionality of generating and retaining data cannot be answered unless we have a good idea of what data is intended, in other words how an "ICR" would need to be generated. This is discussed in greater detail in our evidence to the Science & Technology Committee and that of Dr Richard Clayton and Open Rights Group.

49. After several failures to satisfy all interest groups, it is clear that the Home Office (as advised by private corporations) is merely one interested party in a conflict, and may not have the necessary neutrality and technical expertise to draft legislation to resolve that conflict.

Thank you for your consideration of these comments. This response may be published and attributed, and we would welcome any further questions via our details below.

GreenNet Ltd
Development House
56-64 Leonard St
London EC2A 4LT
Tel: 020 7065 0935
ipolicy@gn.apc.org (PGP fingerprint:1435 8985 F909 CFE7 6F01 E5C0 F50A 699B F041 B0BB)

21 December 2015

[356]See also http://www.thebureauinvestigates.com/2014/11/06/intelligence-agencies-target-and-exploit-legally-privileged-communications-tribunal-hears/ and http://www.theguardian.com/uk-news/2015/mar/13/government-trying-keep-secret-spy-agencies-unlawful-conduct-ipt for one case (Belhaj) that came to light.

Wendy M. Grossman—written evidence (IPB0068)

Summary

Equipment interference as proposed in the draft Investigatory Powers Bill is overbroad and dangerous, placing both individual Britons' lives and the British national infrastructure at risk. Care needs to be taken to limit such powers to devices that are directly used to support human-to-human communications. Consideration should be given to the implications for allocating liability in cases of public safety and criminal prosecutions.

About me

1. I am an award-winning freelance journalist who has specialized in the area of the Internet and related technology for more than 25 years. In that time, I have written books about the developing Internet and have been a regular contributor to the *Guardian*, the *Daily Telegraph*, *Scientific American*, *New Scientist*, and *Infosecurity*, among many other leading publications. In 2013, I won the BT Enigma award for lifetime achievement in security journalism. I am also a member of the advisory councils of the Open Rights Group and the Foundation for Information Policy Research, and the advisory board of Trust in Digital Life.

2. I have been online since 1991, and have covered the internet and related technologies for large and small British and international publications ever since. I wrote one of the first two guides on how to use the Internet for *Personal Computer World* in 1994 and the earliest articles on encryption policy to appear in British publications; more recently, I have worked with academic researchers and written for *Infosecurity* magazine on issues directly relevant to this bill.

What is a computer?

3. The bill proposes to allow interference with "electronic devices such as computers and smart phones". The image this phrasing creates is that of either a self-contained device that is used by one or a few individuals for long-established purposes such as email, word processing, internet browsing, and so on, or perhaps the routers, switches, and other devices that direct data traffic around the internet. This is not the reality of computers today, let alone tomorrow.

4. Modern cars are clusters of computers on wheels - ten to 30 for an ordinary car, as many as 70 for a luxury car.[357] The same or similar is true of other vehicles from tractors to airplanes. Computers are embedded in streetlights in Glasgow,[358] in the smart meters UK electric companies are pledged to roll out by 2020,[359] and in automated vacuum cleaners such as the Roomba and the Dyson 360 Eye,[360] as well as most modern TVs and washing

[357] https://www.infosecurity-magazine.com/magazine-features/cracking-the-computer-on-wheels/
[358] http://www.theguardian.com/public-leaders-network/2015/apr/21/glasgow-the-making-of-a-smart-city
[359] https://www.gov.uk/guidance/smart-meters-how-they-work
[360] http://blogs.wsj.com/personal-technology/2014/09/04/dyson-debuts-first-robot-vacuum-cleaner-the-eye-360/

machines. Computers form an increasing part of toys; for example, Mattel's recent "Hello Barbie", which sends what a child says to it to a remote computer where it can be processed in the interests of formulating a reasonable response. There is even a computer inside every programmable LED light bulb and inside modern medical devices such as pacemakers.

5. As further forms of intelligent, automated machines begin to reach the market, these will contain sensors that collect many more kinds of data than today's domestic devices; they will be on a par with mobile phones except that their embedded microphones, audio, GPS, wifi, accelerometers, and other sensors will be constantly activated as a necessary part of allowing them to function as intended. Simultaneously, the sticker price of such small, deliberately flexible devices as Raspberry Pi and Arduino are dropping rapidly, making adding a computer to such ordinary "dumb" items as door locks, musical instruments, and clothing.[361]

6. Many, if not most, of these sensors will collect data of little interest to security services and law enforcement. Nonetheless, other new sources will be of interest. Even at this very early stage of self-driving cars, law enforcement in the US has expressed an interest in being able to query the location information saved by these cars. Domestic robot companions, such as those being developed in Japan to care for the elderly,[362] will collect particularly intimate data about their owners, including all aspects of their health and home lives. As written, the bill would seem to grant access to all these new sources of data.

7. Does Parliament really intend to grant the intelligence services the right to hack into devices to find out what small children whisper to their favourite toys or study the heart rhythms recorded by individuals' implantable cardiac defibrillators?[363]

The internet of things

8. "Internet of Things" is a broad term describing the expansion of the use of the internet to connect machines and physical objects instead of primarily connecting people. The Internet of Things will take many forms, including smart cities, smart utility grids, and connected robots medical devices, toys, and industrial systems. Many pilot projects are taking place around the world. In Europe, a notable such project has been Smart Santander, a testbed that is currently equipped with about 2,000 deployed devices.[364]

9. Many of our security problems derive from the fact that today's internet is a complex, highly interconnected system. When computers were isolated devices, bugs and vulnerabilities affected only their owners/users. With these computers networked, the same bugs and vulnerabilities have widespread impact across the world and in recent years have resulted in widespread data breaches, cyber attacks, malware deployment, and equipment failures.

[361] http://arstechnica.com/information-technology/2012/12/10-raspberry-pi-creations-that-show-how-amazing-the-tiny-pc-can-be/
[362] http://www.theverge.com/2015/4/28/8507049/robear-robot-bear-japan-elderly
[363] http://www.computerworld.com/article/2492453/malware-vulnerabilities/pacemaker-hack-can-deliver-deadly-830-volt-jolt.html
[364] http://santander.eu

10. IDC predicts that by 2020 the number of connected, autonomous devices that will be part of the Internet of Things will be 30 billion. Most of these devices will be sensors that record information about what's going on around them - time, temperature, location, force - but also may include sensors that collect potentially more personal information such as images and sounds. These streams of information will be sent to more centralized services for processing. Adding the billions of devices expected to make up the Internet of Things will make today's complex, highly interconnected system vastly much more so, making it much harder to understand and secure effectively.

11. Many of the manufacturers of these devices are and will be entering the market for connected devices for the first time. Many will know little about computer security and they will make basic errors. Some will be security mistakes that have long been known in the computer industry; some will be errors of user design that make it hard for tens of millions of consumers to make safe decisions. Much of this poorly designed software will be embedded in devices that are intended to be left in place for many years, even decades. What we have seen so far is an endemic cultural failure to adopt even the most elementary security precautions in protocol, system, and software design or in deployment and operation. Researchers have shown repeatedly that modern cars, medical devices, smart meters, smart parking meters, and baby monitors can be hacked; security issues were promptly found in Hello Barbie.[365]

12. Today's software manufacturers update software for devices such as desktop/laptop computers and smart phones by sending out patches. This model will not work for the Internet of Things. Many of these manufacturers TVs and refrigerators have much longer expected life spans than mobile phones and laptops, and even technically adept people who are used to patching computer software might draw the line at downloading a patch that could turn their £21,000 Toyota Prius into a brick. The vulnerabilities that are embedded in new devices are likely to stay there for the life of the device.

13. The result will be a highly interconnected infrastructure riddled with vulnerabilities that interact in unknown and unexpected ways and that can damage individuals in very personal, even life-threatening ways.

Equipment interference

14. "Equipment interference" is a polite term for "hacking". As written, the bill would appear to authorise two types of government-sponsored hacking: 1) into an individual's devices where there is a warrant; 2) in bulk where there is a warrant and the main purpose is to acquire intelligence about individuals outside the UK.

15. The global nature of the internet and associated technologies makes it unlikely that any device or range of devices can be hacked in such a way that it affects solely British users of those devices. Therefore, a reasonable reading of the bill suggests that UK agents would be authorised to place back doors and other vulnerabilities into widely used

[365] http://www.pcworld.com/article/3012220/security/internet-connected-hello-barbie-doll-can-be-hacked.html

equipment of all types. Such situations are already known; in December 2015 Juniper Networks announced that it had detected unauthorised code inside the operating system used in its network equipment and routers and that the rogue code had likely been in place since at least 2012. This equipment is used by government agencies, large companies, and universities, all of whose encrypted communications are at risk as long as the code is in place (Juniper has issued a patch).

16. It is not possible to create a vulnerability - a hole - in such equipment that only "good guys" or "our side" can use. Adding vulnerabilities to widely used equipment will make Britain's infrastructure vulnerable and aid those who wish to attack Britain by providing additional paths they can use to do it.

17. Further, no hacker, however clever, is perfect. It is entirely possible that in the course of interfering with equipment in order to render it more porous to intelligence personnel, errors will be made. If the equipment being altered is not a network router but , as will increasingly be the case, a computer system that controls the functioning of a physical device whose operation affects the physical world, the danger is to lives, not just bank accounts. Errors may lead to malfunctioning medical devices, crashing the national power grid, crashing planes, or a hundred-car pile-up on the M1, a crashed plane. Even where such damage does not occur, creating a vulnerability in such a system leaves it open to other attackers who wish to cause those effects.

Problems with the bill

18. The bill does not define "computers". In the broadest sense, it could be taken to mean that law enforcement will have the power to hack into any electronic device - which, over time, will mean the majority of physical objects. As written, the bill places people's lives at risk.

19. Granting such powers gives law enforcement a motive not to report bugs and vulnerabilities when they find them. We know from the revelations of Edward Snowden, that the NSA maintains a catalogue of vulnerabilities it can use to plant "back doors" into widely used equipment such as network routers. This practice keeps the global community, including banks, businesses, and medical practices, ignorant of and exposed to the risks they are actually taking and places our entire society at risk, contravening that part of GCHQ's mission that is to protect national security.

20. Granting such powers also creates enormous scope for both the planting of evidence by intelligence agencies and claims they have done so. It will render unreliable established practices of forensic examination. Under such a regime can any verdict that relies on digital evidence be considered safe?

21. A persistent proposal for fixing the problem of insecure software is to require software manufacturers to accept liability for the damage their products cause. This will be particularly important where public safety is involved, such as in the case of self-driving cars and medical equipment, where lives are at stake and damages claims can run into the millions. Allocating legal liability will be impossible if at any time manufacturers can claim

that their equipment was - or could have been - interfered with by government-backed personnel.

22. What Britain does other countries can and do copy. We should be trying to build a more secure infrastructure, not one full of secret holes known only to law enforcement, criminals, drug traffickers, paedophiles, and terrorists.

Suggested remedies

23. The bill should provide greater clarity and limit the types of devices that may be interfered with to those involved in direct human-to-human communications.

24. On the individual level, warrants should be targeted, independently overseen, and proportionate. The future will make it possible to collate a far more intrusive and intimate picture of each individual's life than is currently possible, and limits should be set in advance to ensure that the absence of specific regulation is not taken as an invitation to push the boundaries. The draft code of practice discusses communications, but seems to omit the kinds of data discussed here and their implications.

25. There should be penalties for errors and careless damage as a result of equipment interference activities. In cases of disputed liability, there should be a mechanism for discovering whether government-backed equipment interference has played a role.

26. There should be some consideration given to scrapping the idea of legalising bulk equipment interference. If Britain had a means for punching a hole into the side of every building and vault across the world, everyone would agree it was wrong to use it. That is the equivalent of what's being discussed here.

21 December 2015

Guardian News & Media—written evidence (IPB0040)

About Guardian News & Media

Guardian News & Media (GNM) is the publisher of theguardian.com and the Guardian and Observer newspapers. As well as being the UK's largest quality news brand, the Guardian and the Observer have pioneered a highly distinctive, open approach to publishing on the web and has sought global audience growth as a critical priority. It is owned by Guardian Media Group (GMG), one of the UK's leading commercial media organisations and a British-owned, independent, news media business.

In 2014, the Guardian was named newspaper and website of the year at the Society of Editors UK Press Awards and is the most trusted news source in the UK (Ofcom digital media report, 2014). In May 2015 it won Website of the Year, Editorial Campaign of the Year, App of the Year and Product Team of the Year at the British Media Awards. In December 2015 it won Campaign of the Year, Investigation of the Year and a Guardian journalist was named Foreign Affairs Journalist of the Year at the British Journalism Awards. Its journalistic excellence was also recognised when it became the first news organisation of non-US origin to receive the Pulitzer Prize for its investigation into NSA surveillance. The Guardian is also known for its globally acclaimed investigation into phone hacking, the launch of its groundbreaking digital-first strategy in 2011 and its trailblazing partnership with WikiLeaks in 2010.

Introduction

GNM is pleased to respond to the call for written submissions by the Joint Committee on the draft Investigatory Powers Bill. Following the Guardian's publication of the Snowden revelations, the UK has at times seen a binary debate about the competing public interests of privacy and security, and the legality of the intelligence agencies' activities which the Snowden documents exposed. The stories played a crucial role in highlighting a broad range of public interest considerations and GNM has welcomed the wide range of voices who have argued for the reform of surveillance powers.

As the Committee will be aware, due to the responsible reporting of the Snowden revelations by the Guardian, New York Times, Washington Post and other global news organisations, over the last 18 months, a plethora of legal challenges and independent reviews have questioned existing legislation and intelligence practices. These cases and reviews overwhelmingly demonstrate the need for more transparency, scrutiny, oversight and reform. The Davis and Watson legal challenge and appeal has scrutinised bulk retention of (and access to) communications data and its relationship to the British public's right to respect for private life and protection of personal data under Articles 7 and 8 of the EU Charter of Fundamental Rights. The Court of Justice of the European Union (CJEU) is currently reviewing the case for a final determination of the issues.[366] The June 2015 review

[366] Secretary of State for the Home Department v David Davis MP and others [2015] EWCA Civ 1185, which has recently been referred by the Court of Appeal to the Court of Justice of the European Union where the court asks the CJEU to rule on whether the ground-breaking case of Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural

of the UK investigatory powers regime by Independent Reviewer of Terrorism Legislation David Anderson QC[367] found that the current legal framework is overly complex and disjointed and made a number of significant recommendations. And in February 2015, the Investigatory Powers Tribunal held that GCHQ did indeed act unlawfully by accessing millions of private communications, as collected in bulk in the US, prior to December 2014.[368]

GNM agrees with the Home Secretary's desire to "consolidate existing legislation and ensure the powers are fit for the digital age"[369] . GNM also agrees that UK law enforcement and intelligence agencies must have appropriate powers to keep the citizens of the UK safe. However, these powers must be proportionate, effective, properly authorised and sit within and appropriate oversight framework.

Protections for journalists

The protection of journalistic material, sources and the legitimate activities of journalists is vital to a free press. If sources think they can be identified they will be reluctant to pass on information or to take the risk of disclosure, dismissal or prosecution. Journalistic material must be protected and secure, to enable newspapers to act in the public interest. This is vital to ensuring continual oversight and accountability of the public and private institutions that influence the lives of citizens in the UK. The current legislative framework in the UK - specifically the Police and Criminal Evidence Act 1984 (PACE) - recognises this and sets out a number of protections to protect journalism and safeguard the right to freedom of expression. Crucially, these existing provisions enable journalists and media organisations to make representations to a judge against a police warrant seeking the disclosure of journalistic material.

Part 3 of the draft Bill includes, at clause 61, a requirement for all applications to access the communications data for the purpose of identifying or confirming the identity of a journalist's source to be authorised by a Judicial Commissioner. The draft Bill also requires that statutory Codes of Practice issued in respect of communications data must make provision for additional safeguards for sensitive professions.

However this does not meet the existing standards of set out in PACE, which provides a clear process with proper judicial scrutiny. The draft Bill provides insufficient safeguards for journalism and there is a lack of proper protection for journalistic material and confidential journalistic sources. Communications data can now be obtained for a number of purposes (wider than those previously authorised under PACE) including for any crime (and not just serious ones) (clause 46(7)). These concerns are set out in more detail in the Media Lawyers Association's written submission to the Committee, which GNM endorses in its entirety.

Resources & Others, the case which ruled that European data retention laws were incompatible with Articles 7 & 8 of the EU Charter, also binds national legislators in the making of domestic data retention laws.

[367] https://terrorismlegislationreviewer.independent.gov.uk/a-question-of-trust-report-of-the-investigatory-powers-review/

[368] http://www.theguardian.com/uk-news/2015/jun/22/gchq-surveillance-two-human-rights-groups-illegal-tribunal

[369] HC Deb, 4 November 2015, c969

While the draft Bill (unlike the Regulation of Investigatory Powers Act) includes new protections giving explicit protection to journalists, those protections do not go far enough. Instead, they create a route by which the state can identify a source without going through the much more rigorous safeguards as set out in PACE.

The proposal , under clause 61 of the draft Bill, that there is a requirement for applications to access the communications data to be authorised by a Judicial Commissioner where it is for the specific "purpose of identifying or confirming the identity of a journalist's source" is flawed:

9. Authorisation would happen after the fact - with the judge only able to assess whether the police have "reasonable grounds" for the intrusion - this is merely a review of a police decision, already taken, against an extremely broad standard, that the police may easily be able to make after the fact of disclosure. Furthermore, this weak authorisation process can be bypassed in urgent situations.
10. The authorisation requirement applies narrowly to material where the application is for the purpose of identifying a journalistic source. This wouldn't cover other details acquired by a journalist for the purposes of a sensitive journalistic investigation, or where a source is stumbled upon, for example unpublished material - which is covered under PACE.
11. Applications to the judicial commissioner are made without the knowledge of the media concerned.
12. There is no judicial oversight of data collection involving journalists or journalism if the purpose of the application is for any other reason than identifying a source. It is often the case that identifying a source is collateral or incidental and safeguards need to be in place for those occasions.
13. The proposed procedures outlined in the draft Bill don't apply to applications made to access journalistic communications by the intelligence and security services.

There are also other measures in the Bill which are not targeted at journalists specifically, but which pose a threat to the practice of journalistic more broadly:

16. Encryption of communications is vital to ensure the security of journalistic data and information, including about sources, particularly in the field of investigative journalism. The anti-encryption provisions in Section 118, 4(c)1 of the draft Bill are a dangerous provision, creating an overall weakening of the encryption framework that could lead to third parties being able to access encrypted data more easily. The reality is that once decryption of information is possible for one organisation, it is made possible for other organisations, not least because the creation of encryption keys creates a risk of those keys falling into the wrong hands.
17. The Bill also contains problematic proposals for investigative journalism and protection of sources on "equipment interference", or the capability for security services and the police to remotely hack technology. This permits, for example, the police to access a smart phone and use its microphone covertly to record sound, without the knowledge of the owner. This practice was already being used by the security services, but the parameters will now be defined in statute. A judicial

warrant will be necessary, and a code of practice will be brought in to regulate "the use of more sensitive and intrusive techniques."

18. Part 2 of the Bill relates to the Lawful Interception of Communications. Clause 13 relates to, inter alia targeted interception warrants. Protection for these being used against MPs is included in s 16(1)(b), but there does not appear to be an equivalent protection for sensitive professions such as the legal, medical, journalistic professions. Further, such warrants may be issued in urgent cases (s20) which do not have to be approved by a Judicial Commissioner. Warrants may be modified in quite significant ways (by adding names or premises) and this modification does not require the judicial commissioner to approve it (s26).
19. Part 2 also permits interception of communications in prisons if such a power is conferred under the prison rules (clause 37). However, no provision appears to be made n the draft Bill to protect legal privilege or any such communications with journalists.
20. Part 4 related to the retention of communications data. Part 9 deals with definitions. A telecommunications operator – which is a term which is used throughout the bill – is defined extremely widely, applying to a person who offers or provides a telecommunications services or controls or provides a telecommunications system which is wholly or partly in the UK or controlled in the UK. This definition appears to deliberately bring public and private operators within the scope of the Bill. There are some cases where the Bill appears to refer specifically to public operators but in all other parts of the Bill it applies to both public and private operators (so potentially could apply to the Guardian). It appears that GNM could be caught by this provision. The implications of this for a journalistic organisation are very concerning.
21. Part 5 is about authorizing interference with equipment. Again there are specific measures to protect MPs from this sort of warrant, but none for other sensitive professions such as journalism or the law.
22. Part 6 concerns Bulk interception and acquisition warrants. These bulk interception warrants can sweep up both domestic and overseas material. These also seem to apply to both public and private telecoms providers. Again there are no protections accorded to journalists (not even akin to those conferred in Part 3 under clause 61).

Guardian News & Media
December 2015

Cheryl Gwyn Inspector-General of Intelligence and Security—written evidence

Introduction

1. Thank you for the opportunity to submit this evidence. The submission outlines the functions and powers of the New Zealand Inspector-General of Intelligence and Security (Inspector- General) and how my role relates to other authorisation and oversight mechanisms within the New Zealand system. I hope it may provide useful comparative material to inform the Joint Committee's consideration of the role of the proposed Investigatory Powers Commission.

2. I do not seek to comment on the policy or specific provisions of the Draft Investigatory Powers Bill.

Intelligence and security oversight framework

3. In New Zealand, as in other jurisdictions, the framework of oversight for the intelligence and security agencies has a number of elements and layers:

   3.1 The Directors of the agencies: the Directors authorise the use of certain intellligence- gathering powers against statutory criteria and, when applying to exercise further powers under warrant, must apply on oath.

   3.2 The responsible Minister(s): the Minister in charge of each of the intelligence and security agencies is accountable to Parliament for the general conduct of the agencies. The Minister is also responsible for authorising the exercise of specified intrusive powers, by way of warrant or authorisation.

   3.3 The Minister for National Security and Intelligence: a non-statutory portfolio first assigned in 2014; leads the national security sector and sets the overall framework within which the agencies operate.

   3.4 The Commissioner of Security Warrants: the Commissioner has a joint role with the Minister responsible for the Government Communications Security Bureau (GCSB) in authorising interception warrants or access authorisations if anything is to be done for the purpose of intercepting New Zealanders' private communications and a joint role with the Minister in charge of the New Zealand Security Intelligence Service (NZSIS) for domestic intelligence warrants, where the warrant relates to a New Zealand citizen or permanent resident.

   3.5 The Intelligence and Security Committee (ISC): the ISC is a statutory

committee,[370] rather than a committee of Parliament as select committees are, but its members serve on the ISC in their capacity as Members of Parliament. The ISC consists of the Prime Minister, the Leader of the Opposition, two Members of Parliament nominated by the Prime Minister after consultation with the leader of each party in any government coalition and one member nominated by the Leader of the Opposition, with the Prime Minister's agreement, after consultation with the leader of each party not in government or in coalition with a Government party. The ISC's principal responsibility is to examine the policy, administration and expenditure of each intelligence and security agency.

3.6 The Inspector-General of Intelligence and Security.

3.7 Institutions such as the Controller and Auditor-General, the Privacy Commissioner and the Office of the Ombudsman.

4. The New Zealand intelligence and security agencies can also be, and from time to time are, subject to judicial review and other proceedings before the general courts. There is some specific provision for closed hearings in those courts. There is no New Zealand counterpart to the Investigatory Powers Tribunal.

Role of the Inspector-General of Intelligence and Security

5. The principal external oversight body is my office, the Office of the Inspector-General of Intelligence and Security.

6. The Inspector-General and Deputy Inspector-General are appointed by the Governor-General on the recommendation of the Prime Minister following consultation with the ISC.[371] The Inspector-General's appointment is for a term of three years, with one possible renewal.[372] Removal or suspension from office is by the Governor-General, upon an address from the House of Representatives, for disability affecting performance of duty, bankruptcy, neglect of duty, or misconduct.[373] Leaving aside the term limit, the protections as to grounds and process of removal are similar to those for Judges of the High Court.[374]

7. The role of the Inspector-General was significantly strengthened in late 2013.[375] Previously the Inspector-General had to be a retired Judge, the position was part-time and the Inspector- General had very limited resources and no investigating staff. Under the amendments it became a fulltime role; appointment is no longer limited to former Judges, and the powers and resources of the office now

[370] Intelligence and Security Committee Act 1996 (ISC Act).
[371] Inspector-General of Intelligence and Security Act 1996 (IGIS Act), s 5(2).
[372] IGIS Act, s 6(1).
[373] IGIS Act, s 7.
[374] Constitution Act 1986, s 23.
[375] Inspector-General of Intelligence and Security Amendment Act 2013.

more closely match the mandate.

8. I have held office as Inspector-General since May 2015. I am not a Judge and have not previously held judicial office. Prior to appointment I was a civil litigation lawyer, with fifteen years experience in private practice and ten years acting for the Crown, as Deputy Solicitor- General. I also have experience in a senior public sector policy position.

9. The role of the Inspector-General under the Inspector-General of Intelligence and Security Act 1996 is to "assist" the responsible Minister[376] to ensure that each intelligence and security agency for which he or she is responsible complies with the law. My role is defined functionally, rather than in terms of specific agencies or particular powers. As presently defined, intelligence and security agencies are the New Zealand Security Intelligence Service (NZSIS) and the Government Communications Security Bureau (GCSB).[377] Any other agency may be declared by the Governor-General from time to time by Order in Council as an intelligence and security agency for the purposes of the Inspector-General of Intelligence and Security Act 1996.[378]

10. The Inspector-General does not have a direct reporting relationship to the ISC, but may at any time, with the concurrence of the Prime Minister, report either generally or in respect of any particular matter, to the ISC[379] and the ISC may "consider and discuss with the Inspector- General his or her annual report as presented to the House". The ISC does not have power to request the Inspector-General to undertake an inquiry. The ISC is precluded from inquiring into any matter within the Inspector-General's jurisdiction.[380] I have appeared periodically before the ISC.

Jurisdiction

11. As Inspector-General I have jurisdiction to:

    11.1 **receive complaints** from the public, current and former staff members of the intelligence and security agencies.[381] Complainants must show that they have been or may be "adversely affected" by any act, omission, practice, policy or procedure of the GCSB or NZSIS. Complaints must be independently investigated.[382] The IGIS is also the nominated authority for the purpose of receiving protected disclosures ("whistleblowing") from employees of an intelligence and security agency;[383]

[376] In that sense, the purpose of the role is to strengthen the accountability of the agencies to the executive.
[377] IGIS Act, s 3; ISC Act, s 2.
[378] IGIS Act, s 2. Other agencies that carry out intelligence functions include the National Assessments Bureau (NAB) within the Department of the Prime Minister and Cabinet and the New Zealand Defence Force.
[379] IGIS Act, s 27(7).
[380] ISC Act, s 6(2)(a).
[381] Inspector-General of Intelligence and Security Act 1996 (IGIS Act), s 11(1)(b).
[382] IGIS Act, s 4(b).
[383] Protected Disclosures Act 2000, s 12.

11.2 **initiate inquiries** at the request of the Prime Minister or the Minister responsible, or on my own motion, into the legality and/or propriety of the actions of the intelligence and security agencies.[384] "Propriety" is not defined in the legislation but is clearly intended to have a broader reach than pure legality;[385]

11.3 I am obliged to **report publicly** on all of my inquiries, including inquiries into complaints (subject to security constraints and excepting reports concerning employment matters and security clearance issues).[386] Inquiry reports must be provided to the responsible Minister and the Chief Executive of the agency concerned;[387]

11.4 **review the agencies' internal systems** with a view to certifying annually whether their compliance systems are "sound". In doing so I apply a "positive assurance" approach, that is, I examine what compliance systems and controls are in place; examine a sample of each agency's actions (except in the case of warrants and authorisations, all of which are scrutinised – see below); and apply a materiality threshold;

11.5 **review interception and intelligence warrants and authorisations**. All of the GCSB interception warrants and access authorisations and all NZSIS domestic and foreign intelligence warrants are reviewed. Some of those warrants are selected for deeper analysis – a comprehensive check of the process and path by which the application for the warrant or authorisation was formulated (ie what was the intelligence case and whether other requirements, such as comprehensive disclosure, were met), to the application signed by the Minister (and Commissioner of Security Warrants where required), review and cancellation/non-renewal or renewal of the warrant, what intelligence was collected under it, what use was made of that intelligence, what arrangements were in place for retention and storage, and destruction of the information collected. We make recommendations to improve systems and procedures and sometimes identify a failure to meet the requirements of the legislation.

12. My role is *ex post facto*; I do not have any responsibility for directing or approving operations or warrants. This approach does not preclude the agencies briefing me on planned or ongoing operations. Although it is not my role to approve or authorise, there are situations where prior discussion with my office can help to ensure clarity about the legality and propriety of any planned activity.

13. In my experience there is considerable value in having one oversight body which

[384] IGIS Act, s 11(1)(a),(c),(ca).
[385] See eg Inspector-General of Intelligence and Security Report into the release of information by the New Zealand Security Intelligence Service in July and August 2011, pp 70 & 71, www.igis.govt.nz/publications/investigation-reports/.
[386] IGIS Act, s 25.
[387] IGIS Act, s 25(1).

covers a range of functions, across all intelligence and security agencies. Information and insights obtained in carrying out one function frequently inform another. For example, investigation of specific complaints made by individuals has provided a detailed insight into general operational issues and systemic problems, and I have then been able to take up those general or systemic issues under my wider functions.[388]

14. Likewise, knowledge obtained through my broader oversight functions informs my judgement on complaints. Questions or issues that arise in respect of one agency may inform my approach in respect of the other agency. While New Zealand's intelligence and security agencies are understandably small in scale, their activities are nonetheless complex and raise many of the same issues faced by such agencies in larger jurisdictions. The breadth of functions and powers under the IGIS Act enables me and my staff to acquire and maintain a comprehensive understanding of those activities.

Rights of access; investigative and remedial powers

15. The Inspector-General's powers are coupled with a right of access to all security records held by the agencies and a right of access to all of the agencies' premises, ICT systems and staff.[389] The *quid pro quo* for that privileged access is that my staff and I are subject to the same constraints on receiving, holding and using classified information as are intelligence and security agency staff. We must all be security cleared to the highest level. Security clearance vetting is carried out by the NZSIS, which has the statutory mandate to conduct all vetting. We work in a SCIF (secure compartmented information facility) and follow the same security measures as agency employees.

16. In the case of inquiries, I have strong investigative powers akin to those of a Royal Commission, including the power to compel persons to answer questions and produce documents and to take sworn evidence.[390] My proceedings, reports and findings are challengeable only for lack of jurisdiction.[391]

17. I have recommendatory powers only, including the recommendation of remedies that involve the payment of compensation.[392] In addition to the persuasive effect of my findings at the level of the agencies themselves, Ministers and/or the public and the possibility of indirect enforcement by court proceedings based on an inquiry report, the IGIS Act also specifically provides that, where I have made recommendations, I can subsequently report further on whether those recommendations have been met.

[388] For example, individual complaints concerning NZSIS security clearance assessments led to the identification of a recurrent question of whether the procedures followed by the NZSIS in making its assessments and recommendations were consistent with the legal obligation of procedural fairness: see Annual Report for Y/E 30 June 2015, at pp 15-18, www.igis.govt.nz/publications/annual-reports/.
[389] IGIS Act, ss 20 & 21.
[390] IGIS Act, ss 23 & 24.
[391] IGIS Act, s 19(9).
[392] IGIS Act, s 11(6).

Public education

18. It is also, in my view, part of the Inspector-General's role to help the public to understand the powers and activities of the agencies – and the limitations and controls on those powers. To that end, in addition to publishing reporting on all inquiries, my office has a website (www.igis.govt.nz) and a Twitter address (@igisnz) and I look for opportunities for public engagement to talk about the work of the office.

19. It is not for the Inspector-General to seek to increase public confidence in the agencies but if, over time, the public can see that there is robust and independent oversight and that the agencies and their Minister(s) respond to criticisms and recommendations, then one would expect public confidence to grow.

Funding, staffing and administrative support

Funding

20. The Inspector-General's office is funded through two channels. The first is a Permanent Legislative Authority (PLA) for the remuneration of the Inspector-General and the Deputy Inspector-General.[393] The second is the operating costs of the office which are funded from Vote: Justice (Equity Promotion and Protection Services), as part of the Ministry of Justice's non-Ministry appropriations.

21. Pursuant to Cabinet direction the capital costs of establishing the expanded IGIS office (following the 2013 legislative changes) and its operational costs were funded from reprioritising existing New Zealand Intelligence Community baselines. It would not be appropriate in the longer term for the agencies which are being monitored to have to fund the oversight body.

Staffing

22. The Inspector-General may appoint such staff as necessary, but must consult with the Chief Executive of the Department of the Prime Minister and Cabinet as to staff salaries and allowances.[394] My office currently comprises the Inspector-General, Deputy Inspector-General, four Investigating Officers, an IT Manager/Security Advisor and an Executive Assistant/Office Manager. All are fulltime roles. Of the current Investigating Officers, one is employed on a permanent basis and three are seconded from other government agencies (New Zealand Police, New Zealand Customs Service, Inland Revenue). The secondments have enabled me to procure a range of essential investigative and analytical skills.

[393] IGIS Act, s 8.
[394] IGIS Act, s 10(2).

23. Effective oversight of the agencies' use of current and developing technologies requires a sufficient understanding of those technologies by the oversight body, whether through the knowledge and expertise of our own staff or by access to external technical experts. My office has an IT expert but we also rely on agency expertise. While the agencies are generous with their time it is important for the credibility of the Inspector-General's office as an independent oversight body, and the ability to ask necessary searching questions, that we continue to develop our own knowledge and expertise.

24. The current operating costs of the office are approximately $1.5m per annum in total, including staff costs and the cost of operating secure systems and premises. As at May 2015 when I discussed this question with the ISC, a crude calculation indicated that the Inspector- General had the equivalent of just under 1% of the staff and budget of the two agencies for which I have oversight responsibility. That percentage remains at a similar level. It is not fixed in policy or in legislation.

Advisory panel

25. I am supported by a two member statutory advisory panel.[395] The panel members have appropriate security clearances to enable them to have access to, and discuss with me, the classified material held by the NZSIS and the GCSB that my office must consider in order to carry out our review, inquiry and audit functions.

Administrative support

26. Ongoing administrative support, including finance and human resources advice, is provided to the Inspector-General's office by the Ministry of Justice. The New Zealand Defence Force provides standalone secure offices (separate from the agencies' premises) and also provides IT support, both on a cost recovery basis.

11 January 2016

[395] IGIS Act, ss 15A-15F. The members of the panel are Christopher Hodson QC (chair) and Angela Foulkes.

Dr Christian Heitsch—written evidence (IPB0111)

Introduction

1 My name is Dr Christian Heitsch. I am a law lecturer at Brunel University London and a member of the Brunel Centre for Intelligence and Security Studies. I have several times presented at academic conferences about legal issues of bulk cyber surveillance. In 2011, I attended a Chatham House event about the Justice and Security Green Paper.

2 This submssion considers the Draft Investigatory Powers Bill (henceforth: 'DIPB') from a constitutionalist, human-rights-based perspective and will explain why the assumption that the DIPB's clauses about bulk powers are compatible with the Human Rights Act 1998 and / or the European Convention on Human Rights is open to reasonable doubt.

Proposed bulk powers and human rights law

3 It is submitted that the proposed bulk powers and their authorisation regime are incompatible with human rights law. This relates to the DIPB clauses about bulk interception, bulk acquisition of communications data, bulk equipment interference warrants and bulk personal data set warrants.

The German G 10 Act as a template for a human-rights-compliant regime

4 The leading case about the compatibility of bulk surveillance powers with article 8 of the European Convention on Human Rights is *Weber and Saravia v. Germany*.[396] The ECtHR ruled that a challenge to the German G10 Act, that is the authorisation regime for the strategic interception and evaluation of telecommunications was manifestly unfounded and therefore inadmissable. To justify its finding that the German regime was 'in accordance with the law' for purposes of article 8(2) of the European Convention on Human Rights, the Strasbourg Court pointed to the following characteristics of the relevant German statute (*Weber*, at paras 96 *et seq.*):

- The German G 10 Act expressly enumerated the exact offences for the prevention of which the stategic interception of telecommunications could be authorized;

[396] *Weber and Saravia v. Germany*, Application no. 54934/00 (ECtHR, 2006)

- The conditions for strategic monitoring as laid down in the G 10 Act indicated which categories of persons were liable to have their telecommunications monitored;
- The maximum duration of strategic monitoring measures was three months: the implementation of the measures could be prolonged for a maximum of three months at a time, as long as the statutory conditions for the order were met;
- The procedure to be followed for examining and using the data obtained was regulated in detail. In particular, the German Act laid down limits and precautions concerning the transmission of data to other authorities;
- The Act set out in detail the procedure for the destruction of data obtained by means of strategic monitoring: The authorities storing the data had to verify every six months whether those data were still necessary to achieve the purposes for which they had been obtained or been transmitted. If that was not the case, the data had to be destroyed and deleted from the files or at the very least access to them had to be blocked. The destruction had to be recorded in minutes and in some cases be supervised by a senior official – a staff member qualified to hold judicial office.

5 By contrast, the clauses of the DIPB about the authorisation bulk measures do not enumerate the offences for the prevention of which the powers may be used. Rather, the DIPB permits the relevant warrants to be issued

> *'in the interests of national security; or on that ground [and] for the purpose of preventing or detecting serious crime, or in the interests of the economic well-being of the United Kingdom in so far as those interests are also relevant to the interests of national security.*[397]

6 The DIPB lacks any definition of national security and its definition of serious crime (clause 195) appears to be significantly less detailed than the equivalent provisions of the German G 10 Act.

[397] E.g. DIPB, clause 107(1)(b) read in combination with clause 107(2)

7 Further, the maximum duration of any warrants under the DIPB is six rather than three months.

8 Lastly, the procedures for evaluation, transmission, and deletion of data obtained by way of bulk measures are not set out in the DIPB itself. Rather, the Secretary of State is tasked with preparing the requisite 'arrangements' for these matters.

9 In *Weber and Saravia*, the European Court of Human Rights also held that the German G 10 Act was compatible with the requirement of article 8(2) ECHR that any interference with the right to respect for private life and correspondence must be 'necessary in a democratic society'. To justify this finding, the Court pointed to the following additional characteristics of the German law (at paras 115 et seq.):

- Bulk interception of telecommunications could be ordered only on a rasoned application and if the establishment of the facts by another method had no prospect of success or was considerably more difficult;
- The decision to monitor had to be taken by the responsible Government Minister who had to obtain prior authorisation from the independent G 10 Commission or, in urgent cases, ex post facto approval;
- The safeguards with regard to the implementation of bulk interception and the processing of the data obtained had been spelled out in detail. Most importantly, such data had to be marked as stemming from strategic monitoring and were not to be used or transmitted for ends other than those listed in the statute;
- The German G 10 Act established the G 10 Commission which had to authorise bulk interception and had substantial power in all stages of the process.

10 The current version of the G 10 Act in its section 15(5) expressly provides that the G 10 Commission

> *'shall ex officio or in response to complaints submitted to it rule on the legality and necessity of interception measures.*

11 In accordance with traditional principles of German administrative law, the G 10 Commission has the power to review *de novo* the Minister's order authorising bulk interception. This is a quasi-appellate jurisdiction giving the Commission the right to substitute its own view as to whether a measure is legal and necessary for that of the Minister.

12 By contrast, the DIPB includes no express and stringent 'last resort clause' to the effect that bulk measures may be taken only where the applicant intelligence service has demonstrated that the establishment of the facts by another method has no prospects of success or would be considerably more difficult. Rather, the DIPB has weak language to the effect that the 'factors to be taken into account when considering whether the conditions [of necessity and proportionality] are met include whether the information which it is thought necessary to obtain under the warrant could be obtained by other means.'[398]

13 Also, the DIPB continues to grant to the Secretary of State the power to issue warrants authorising bulk measures. There is only a weak justification for vesting these powers in Secretary of State. This is because in practice the accountability of the Secretary of State to Parliament for the activities of the intelligence services is significantly diluted: It is generally acknowledged that Ministers may – which means that they in practice inevitably will – refuse to answer Parliamentary questions on the grounds of national security.[399] Indeed, the Ministerial Code expects

> *'Ministers [to] be as open as possible with Parliament and the public, refusing to provide information only when disclosure would not be in the public interest, which should be decided in accordance with the relevant statutes and the Freedom of Information Act 2000[.]*[400]'

14 The Freedom of Information Act 2000, section 23(1) declares information held by public authorities to be exempt from disclosure 'if it was directly or indirectly supplied to the public authority by, or relates to, any of the bodies specified in subsection (3), i.e. among others, MI5, MI6 and GCHQ. In addition, section 24(1) of the Freedom of Information Act

[398] E.g. clause 107(5) of the DIPB
[399] Mark Sandford '*Parliamentary Questions: recent issues*' House of Commons Library briefing paper No. 04148, 6 May 2015, p. 7
[400] Cabinet Office, Ministerial Code, October 2015, para. 1.2 d

2000 renders exempt from disclosure any 'information which does not fall within section 23(1) […] if exemption from [disclosure under the Freedom of Information Act] is required for the purpose of safeguarding national security.' The Freedom of Information Act also provides that a certificate signed by the Secretary of State stating that information is exempt under sections 23(1) or 24(1) 'shall […] be conclusive evidence of that fact.' Thus, *mutatis mutandis*, the Secretary of State may refuse to answer any parliamentary question 'which directly or indirectly relates to' MI5, MI6 and GCHQ', or in regard to which the Secretary of State simply makes a statement to the effect that refusing a response is required for the purpose of safeguarding national security.

15 In *Liberty v. UK*,[401] the European Court of Human Rights contrasted the provisions of the Interception of Communications Act 1985 ('ICA 1985') about the interception of external telephone communications with the German G 10 Act; the Court ruled that the Interception of Communications Act was incompatible with article 8 of the European Convention on Human Rights. Importantly, the ICA 1985 set the template for the British regime for the authorisation of bulk interception and surveillance powers – a template which the subsequent provisions of the Regulation of Investigatory Powers Act 2000 ('RIPA 2000') as well as the relevant clauses of the DIPB have faithfully copied. Admittedly, the Investigatory Powers Tribunal recently held that, for the most part, the current UK practice of bulk surveillance under the uniform ICA 1985 / RIPA 2000 / DIPB legal template was compatible with the Human Rights Act 1998.[402] However, in my considered view the recent submission of the human rights organisations[403] challenging those judgments of Investigatory Powers Tribunal in the Strasbourg Court does make a very plausible argument that the Investigatory Powers Tribunal's opinion in this regard was flawed.

Cumulative effect of bulk powers on privacy

16 Furthermore, the cumulative effect of the bulk powers included in the DIPB casts additional doubt on the Bill's proportionality. The combination of bulk interception of

[401] *Liberty and others v. the United Kingdom*, application 58243/00 (ECtHR, 2008)
[402] *Liberty and others v. Security Service, SIS and GCHQ*, case no. IPT/13/77/H (Investigatory Powers Tribunal, 05/12/2014, 06/02/2015, and 22/06/2015)
[403] Available from https://www.amnesty.org/en/documents/ior60/1415/2015/en/ (accessed 21/12/2015)

communications, bulk access to communications data, bulk equipment interference, and bulk access to personal data sets mutually reenforces each power's effect on privacy.

17 Also, the combination of bulk powers appears to lay the foundations for a British version of 'Total Information Awareness'[404] – that is permit access by the intelligence services to any lawfully available data with a view to applying data mining and pattern recognition software to prevent acts of terrorism. There is some indication this is inded what is being intended.[405]

18 The assumption that this strategy is more suitable for preventing terrorism than targeted surveillance appears to be manifestly flawed. Security expert *Bruce Schneier* has made an argument that mass surveillance 'can't, won't and never has stopped a terrorist.' In his view this is because the mathematics of pattern recognition techniques inevitably produce an overwhelmingly large number of false positives each of which would need to be investigated which in turn leads to ineffective use of staff and a wasted effort; because terrorist attacks are extremely rare and each attack is unique which leads to each successful attack having an unduly high impact on the detection criteria used subsequently; and because serious adversaries tend to be sophisticated in their ability to avoid surveillance.Targeted measures alone very likely would be more effective.[406] A legal regime's clearly demonstrable unfitness for purpose is one of the factors Courts will use when rueling on that regime's proportionality.

Effective rubber-stamping role of the proposed Judicial Commissioners

19 The new Judicial Commissioners effectively have a rubber-stamping role. This is because they are to apply standards of judicial review rather than have a quasi-appellate jurisdiction when confirming warrants issued by the Secretary of State. The grounds for judicial review most likely are those set out in Council of Civil Service Unions v. Minister for the Civil Service:[407]

---

[404] 'Total Information Awareness' was an - officially discontinued – programme of the U.S. National Security Agency and Defense Advanced Research Projects Agency for the development of, among other things, data search and pattern recognition techniques to predict and preempt acts of terrorism. For basic information, see The Information Warfare Site, http://www.iwar.org.uk/news-archive/tia/total-information-awareness.htm (accessed 21/12/2015)

[405] Sir David Omand, '*The National Security Strategy: Implications for the UK intelligence community*', February 2009, p. 9, available from http://www.ippr.org/publications/the-national-security-strategy-implications-for-the-uk-intelligence-community (accessed 21/12/2015)

[406] Bruce Schneier *'Why Mass Surveillance can't, won't and never has stopped a terrorist'*, available from http://digg.com/2015/why-mass-surveillance-cant-wont-and-never-has-stopped-a-terrorist (accessed 21/12/2015)

[407] *Council of Civil Service Unions v. Minister for the Civil Service*, [1985] AC 374, at 410 *et seq.* (Lord Diplock)

- Illegality in the sense that 'the decision-maker must understand correctly the law that regulates his decision-making power and must give effect to it';
- Irrationality – 'a decision which is so outrageous in its defiance ofl ogic or of accepted moral standards that no sensible person who has applied its mind to the question to be decided could have arrived at it';
- Procedural impropriety – 'failure to act with procedural fairness towards the person who will be affected by the decision' as well as 'failure to observe procedural rules expressly laid down in the legislative instrument by which [the decision-maker's] jurisdiction is conferred'.

20 Where an interference with a Convention Right within the meaning of the Human Rights Act 1998 is at issue, there now is a distinct fourth 'header' of judicial review, namely proportionality. Proportionality review is an investigation into:[408]

- Whether the public policy objective being pursued is sufficiently important to justify the interference with a Convention Right;
- Whether the means chosen to achieve the objective is rationally related to it;
- Whether the interference with the Convention Right is no more than what is necessary to achieve the objective;
- Whether a fair balance has been struck between the interests of the person affected by the administrative decision and the interests of achieving the public policy objective.

21 Outside the ambit of EU and ECHR law, proprotionality can provide structure to irrationality review, by pointing to factors such as suitability or appropriateness, necessity and the balance or imbalance of benefits and disadvantages.[409]

22 Given the vague language of the DIPB clauses authorising bulk measures, the wide scope of the grounds justifying such authorisations, and the option of defining 'general operational purposes',[410] the Secretary of State will easily be able to avoid a finding by

[408] *Huang v. Secretary of State for the Home Department* [2007] UKHL 11
[409] *Kennedy v. Charity Commission* [2014] UKSC 20; *Pham v. Secretary of State for the Home Department* [2015] UKSC 19
[410] Clauses 110, 122, 125 and 140 of the DIPB

Judicial Commissioners that an authorisation is illegal, irrational or in breach of procedural requirements.

23 When reviewing authorisations of bulk measures for proprotionality, the Judicial Commissioners will likely take a somewhat deferential approach, that is give some weight to the judgment of the Secretary of State while engaging in some degree of scrutiny of his or her decisions. This approach would reflect recent case law.[411] Ultimately, it will in most cases be the Secretary of State whose views on the necessity, proportionality and legality of bulk measures will be determinative.

21 December 2015

[411] *A and others v. Secretary of State for the Home Department* [2004] U.K.HL. 56

Dr Tom Hickman—written evidence (IPB0039)

The "double lock"

1. The Bill retains the responsibility of the Secretary of State for the decision to grant a warrant in all cases, but a Judicial Commissioner ("JC") will now ensure that a warrant is lawful. The approach is justifiable in my view.

2. Granting warrants can involve political considerations and risks that are appropriate for the Secretaries of State to consider, particularly in cases touching on foreign policy, high profile individuals (tapping of foreign diplomatic phones, to give one example), and in other sensitive cases.

3. Admittedly wider considerations are less prevalent, but not necessarily absent, outside the national security and foreign policy arena and here the case is stronger for placing approval solely in the hands of judges.

4. The fact that warrant requests go through the Secretary of State's office and must be signed off by the Secretary of State personally also imposes a discipline and instills a caution on the part of public officials answerable to the Minister, which is not always present with a judge. Indeed, a real problem in my view with putting decisions in the hands of judges is that it off-loads responsibility from the shoulders of public officials and tempts them to adopt an attitude of 'if its good enough for the judge its good enough for me'. Since judges inevitably pay considerable deference to public officials, this can lead to a protection gap.

5. The objection that some have already raised about the double lock is that it will engender greater deference on the part of the JCs. However, the fact that the JCs will be mandated to apply judicial review principles does not mean that they will apply a *Wednesbury* review. It is trite law that in human rights cases courts will decide for themselves whether a measure is necessary and proportionate and these are the judicial review principles that judges will surely adopt (e.g. *Miss Behavin' Ltd* [2007] 1 WLR 1420).

6. The reference to judicial review principles is thus unfortunate in terms of clarity, and preferably these words would simply be deleted. However upon analysis it should not be of significance in substance.

7. It is much more important for enhancing judicial scrutiny is tightening the objectives for which warrants can be issued and requiring greater specificity as to the proposed use of material obtained under the warrant, introduction of counsel to JCs, as well as preventing executive amendment of warrants.

8. In my view, the Bill certainly needs to have a provision for special counsel to JCs. Judges are used to hearing argument on both sides and evaluating their respective strengths. The danger with introducing JCs without the ability for argument on both sides is that there will be little meaningful scrutiny beyond a fairly formal assessment

of the application and identification of obvious deficiencies.

9. This would not be a special advocate function but Counsel to a JC. Special advocates represent the interests of an individual and they are able to take instructions from that individual (freely before they have seen closed material and thereafter without being able to respond without permission). There would be no such ability to take instructions in order to represent the interests of a specific person under the Act.

10. Counsel to a JC would enable arguments to be developed as to why a warrant request goes too far or is inadequately supported etc. This will enhance judicial scrutiny and ensure that the ability to refuse to approve a warrant is more meaningful. The use of such Counsel in every case may be impractical. But they should certainty be available to JCs and one can envisage their use routinely in controversial cases on the boundaries of 'national security', in cases involving journalists and lawyers and major operations, in cases which rely on a broad meaning of the Act or which test key provisions, and in many other cases in which a JC perceives some issue on which he or she would appreciate contrary argument being put forward.

Thematic warrants

11. RIPA provides very clearly that domestic interception warrants are to be targeted at *"one person as the interception subject"* or *"a single set of premises"* (s.8(1)(a)).

12. Despite this, the ISC has revealed that MI5 has in fact been obtaining what are called *"thematic warrants"* which relate to *"any organisation, association or combination of persons"*. This surprising approach derives from the very broad definition given to the word "person" set out at the back of the Act.

13. It is far from self-evident that it was Parliament's intention to authorize thematic warrants under RIPA. It is not clear from the face of section 8. The expansion of the terms of that section is by reference to an interpretation clause which is general in nature, applying to the whole Act, and not obviously intended to expand that specific power. Moreover, such an extension cuts across deeply entrenched principles of the common law.

14. A foundational series of eighteenth century cases established that the use of "general warrants", which permitted arrest and search and seizure in respect of classes of individuals, usually the *"authors, printers and publishers"* of a named periodical, were unconstitutional. Henceforth, the need to identify suspects or specific property was a basic touchstone of the warrant system. The offensiveness of general warrants is that they delegate to those executing the warrants authority to determine the strength of evidence against individuals and thus whether they are subject to the coercive authority of the warrant or not. As Lord Mansfield stated in *Leach v Money* "*It is not fit, that the receiving or judging of the information should be left to the discretion of the officer. The magistrate ought to judge…"* (IXX St Tr 1021, at 1027).

15. The Grand Chamber in the very recent judgment in *Zakharov v Russia* (47143/06), 4

December 2015, made clear that this approach is also required by the ECHR: *"the interception authorisation, … must clearly identify a specific person …or single set of premises"* (at [260], [264]).

16. Worryingly the Interception of Communications Commissioner's Office said in evidence to the ISC that it felt that the use of thematic warrants had been abused. It is precisely because of abuse of the system which led to general warrants being outlawed.[412]

17. Regrettably, cl.13(2) of the Bill follows the dubious approach taken under RIPA, allowing a warrant to be obtained in respect of*, "A group of persons who share a common purpose or who carry on, or may carry on, a particularly activity"*. Since it does not require such individuals to be named (or even known) this is equivalent to the general warrants outlawed 250 years ago.

18. A so-called targeted warrant could therefore be granted for all persons who are believed to support ISIL as they *"share a common purpose"*. Or it could be granted for persons who may wish to conduct a terrorist attack in London, since such persons may carry on a particular activity, or in respect of attendees at a meeting, demonstration or summit.

19. It is also unclear whether the reference to "group" means an existing association of persons or not, and if so how close that association should be (should they all know each other or be in contact now or in the future?).

20. Targeted warrants are at the heart of the interception regime. It is extremely important in principle, and in conformity with common law and ECHR authority, that:

    (1) Such a warrant is limited to specified persons or places (a single warrant can contain more than one, but they must be specified).

    (2) It is as clear as possible what is embraced in such a warrant. The current draft is vague and open to a very expensive interpretation.

Modification of warrants

21. It is entirely inappropriate for modification of a warrant that has been approved by a JC to be made without requesting such a modification from the JC him or herself. If it is necessary, as it will be, for conditions such as the persons to whom a warrant applies to be specified and approved by a Judicial JC it is illogical and subversive of the whole scheme of judicial authorisation for those approved conditions to be capable of being changed without reference back to the JC.

22. It should also be noted that the modification that would be permitted by cl. 26(2)(a),

[412] For discussion of the cases and the abuse, see T. Hickman "Revisiting Entick v Carrington: Seditious Libel and State Security laws in Eighteenth Century England" in A Tomkins and C Scott, *Entick v Carrington - 250 years of the rule of law* (Hart 2015).

"adding or removing the name or description of a person, organisation of set of premises" has to be read with the definitions section in clause 195 which defines person as "any association or combination of persons". Thus, a warrant for use in against association A, say, a radical Muslim association with feared terrorist connections, could be modified to add an entirely different muslin group, or even an entirely unconnected association or even loose affiliation of persons without judicial approval. This is not only unprincipled under a regime of judicial approval, but could easily be open to abuse as a means of embracing more controversial extensions of a warrant that it was thought might not pass judicial muster.

23. Moreover, "varying" a name or description of a person, group, association or combination of persons (cl. 26(2)(b)), is not necessarily a "minor" matter, as the draft Bill states. A warrant to intercept communications of "persons demonstrating outside the Embassy of Country X" could for instance be modified to intercept the communications of persons demonstrating outside Embassy B, or other locations, thus changing entirely the character of the warrant and considerations directly related to the necessity and proportionality of the warrant. Any modifications must have judicial approval.

Bulk interception warrants

24. The breadth of the power to grant non-targeted interception warrants for the purpose of intercepting "external" communications only became apparent in 2014 during the IPT proceedings brought by several NGOs against the Government, following Snowden's disclosures.

25. The case drew attention to three features of the power:

(1) First, the Government has treated interactions with foreign internet servers to be external communications and thus capable of being the target of such warrants. In evidence in the IPT proceedings, the Government described how a person's interactions with services such as Twitter, Facebook and Google pages hosted on US servers are regarded as external communications and obtaining such data can thus be amongst the purposes of a bulk interception warrant.

(2) Second, bulk interception warrants are effected by tapping fibre optic cables, and since a huge amount of domestic internet traffic (such as UK-UK emails) is routed via the US, such data are regarded as fair game as a necessary incident of the power.

(3) Thirdly, the growth in the amount of communications data available on individuals has meant that it is this, rather than the content of communications, which is the principal object of interest of the intelligence services. The extra safeguards in RIPA for bulk interception, namely that where a person of interest is based in the UK a targeted warrant must be obtained, only applies to content data: there is no equivalent statutory protection for non-content data about persons in the British Isles (the Bill is the same: cl. 119(1)(c), (4)).

26. The consequence is that under the bulk collection power the intelligence services have been obtaining huge amounts of very revealing data about persons in the UK which can be accessed for the general statutory purposes of national security and fighting serious crime.

27. This very broad power is continued in the Bill. Cl. 111(3) of the Bill provides that: *"A bulk interception warrant must specify the operational purposes for which any intercepted material or related communications data obtained under the warrant may be selected for examination*."

28. The Bill states that it is not sufficient to simply specify *"national security"* or *"*serious *crime"*, but it adds that, *"the purposes may still be general purposes"* (cl.111(4)). Therefore the Bill would still authorise interception and examination of data for very general purposes such as tackling the ISIS threat or drug-trafficking, which some, but not enough, control on its use.

29. At a minimum in my view the Joint Committee should insist on:

    (1) Tighter protections for persons in the UK particularly in relation to use of communications data requiring at least operationally independent authorization for use of such data together with JC approval where this would be required for police obtaining communications data.

    (2) Requiring warrants to be more narrowly focused as to their purpose and permitted search criteria. The Act could require that the purposes will be specified as tightly as is operationally reasonable.

    (3) Bringing safeguards currently in the Code to legislation and other matters on record-keeping and destruction from internal policy to legislation.

Code and Internal Policies

30. The Code itself is not legally binding and currently no draft Codes have been published along side the Bill.

31. The Committee should make sure that all protections it considers necessary are set out in statute as a requirement of the law, if necessary in a Schedule to the Bill. In such an important area it is not appropriate for important matters to be regulated by "soft law".

32. The argument that may have justified such an approach under RIPA, that breach of less important protections should not be regarded as the unlawful obtaining or use of data has never been persuasive. It has lost all of its traction now that the Code is part of the "according to law" requirement under Article 8, such that violations will result in obtaining or use being contrary to Article 8 and thus unlawful under the Human Rights Act 1998.

33. Internal policies are not only, as with the Codes, not legally binding, but they are not independently created, are not open to Parliament and citizens to inspect and are, essentially, merely advisory and open to change and amendment at any time by the department or agency concerned.

34. Whist internal policies might properly address matters of pure internal departmental or agency procedure or organisation, specific to the department or agency in question, it is not appropriate for internal policies to replicate, in different language, the Act or Code, which applies to all public bodies exercising relevant powers and is made under statue, although it appears from recent IPT cases that this is what has happened in practice in the intelligence agencies. That is a recipe for confusion and watering-down of Code and legislative standards.

35. The tendency, revealed in the IPT proceedings, for substantial matters relating to record-keeping and document retention and destruction, as well as approvals for the use of data, to be dealt with in internal policies should be curtailed by Parliament. Likewise, the use of extensive Codes that sit under the legislation but have ambiguous status and effect should be greatly reduced. All necessary protections should be set out in law.

36. Therefore insofar as any stipulations are required by Parliament as a protection for individual privacy, such matters should be embodied in the Bill.

Communications data

37. It is now becoming widely accepted that, when aggregated, communications data are more revealing and intrusive then content data – identifying a person's contacts and associations, websites visited (up to the first slash), providing information about habits and preferences and even tracking a person's movements.

38. Yet the massive demand from police and intelligence agencies for rapid and large-scale access to such data may make the imposition of equivalent safeguards to content data politically unfeasible, however desirable in principle.

39. Under the Bill:

    (1) There is a change to the meaning of communications data. This would now include any data "which identifies or describes an event (whether or not by reference to its location)" or information which is about "an entity". Events data and entity data can be data derived from content although cannot disclose its meaning (cl. 193(1)-(6)). Presumably, this would mean that voice or other identity recognition traces that can be derived from a communication are not protected as content data. (Could data recognition software be run on internet communications without "intercepting" content data?) – the Joint Committee should be clear as to how far non-content powers range.

(2) Second, obtaining communications data would remain largely – but no longer exclusively – outside the warrant regime. The requirement for a designated senior officer who approves such requests to be independent of the investigation would be given statutory force (cl. 47(1)) as well as a requirement for consultation with a Single Point of Contact, a specially trained person within a public body who essentially acts as a compliance officer (c. 60). Both are welcome changes. However, this could be taken further, for example by requiring or empowering Single Points of Contact to make references to JCs or, as indicated by the CJEU in Digital Rights Ireland, requiring institutionally independent authorisation.

(3) Third, there is no justification for exempting the intelligence agencies from these important protections.

Communications data: extension of judicial warrants

40. The requirement for Judicial Commissioner approval should be extended beyond journalistic material to communications of journalists, lawyers, ministers of religion, members of parliament and doctors, as well as in relation to more sensitive data like movement information. If bulk communications warrants are permitted, this should extend to examination of material obtained under such a warrant.

41. In respect of legal professional privilege, it is now well established that communications data can:

(1) Reveal the content of communications, by reference to the timing and nature and frequency of contact, and such information can be subject to LPP for that reason.

(2) Disclose information which is capable of attracting legal privilege about the identity and whereabouts of a lawyer's client. The reason such information attracts legal privilege is because, in cases where such information is confidential, it would interfere with a person's right to uninhibited access to a lawyer to make such information capable of disclosure.

42. Indeed, it is striking that the intelligence agency "Arrangements for the Acquisition of Bulk Communications Data" which have now been published, state:

"In all cases where Intelligence Service staff intentionally seek to access and retain BCD relating to individuals known to be members of the professions referred to above [medical doctors, lawyers, journalists, Members of Parliament, Ministers of religion], they must record the fact that such communications data has been accessed and retained and must flag this to the Interception of Communisations Commissioner at the next inspection." (page 6).

43. This guidance acknowledges (1) that all of the stated professions call for special

protection, (2) that the protection is required in respect of requests to obaain communications data relating to such individuals (i.e .it is not necessary to show that it was for the purpose of identifying journalist sources, legally privileged material or other highly confidential material), and (3) that such access justifies judicial oversight, hence, the reference to flagging to the Judicial Commissioner.

44. This protection should be moved from guidance into statute, not only in relation to bulk collection of communications data (if permitted) but in relation to obtaining communications data generally.

Bulk collection of communications data

45. The biggest revelation (made in information supplied with the Bill) is that MI5 and GCHQ have been using a very generally worded power contained in s.94 of the Telecommunications Act 1994 ("TA 1984") to *"give …directions of a general character"* to telecommunications companies, in order to obtain communications data in bulk from such companies, scooping up vast amounts of data on persons both outside *and also inside* the British Isles.

46. The Bill would abolish s.94 and require a proper legal basis under the warrant regime for this power. But in common with bulk interception warrants, examination of the data would be permitted as long as it is *"for the specified purpose"* (132(1)) and the purposes for which the warrant could be granted could be very general purposes, such as the fight against drug trafficking, child exploitation or ISIS (c. 125)

47. This is the most concerning issue raised by the Bill (and there are many concerning issues). The breadth of the power, allowing the intelligence services to search within very broad search parameters the communications data of everyone in the UK is breathtaking. The fact that a JC would be required to approve a bulk warrant provides little comfort.

48. Non-statutory "arrangements" for the acquisition of bulk communications data under s.94 have now been published which refer to a *"strict authorisation process"* for accessing the data. But there is no requirement for operational independence in approvals, still less is such a safeguard proposed to be given the force of law. This authorization process is regulated by internal policies – it is self-authorisation.

49. It is very unlikely that this would be regarded as Article 8 compatible by either the European Court of Human Rights of the European Court of Justice.

50. Since requests for communications data by other public bodies can be made in broad terms, it is difficult to see that there is a compelling justification for exempting the intelligence services from the communications data authorisation regime. Suggestions for tightening that regime have been made above.

Internet Connection Records ("ICR")

51. ICR are data that identify when a device used an internet service or visited a webpage

(up to the first slash).

52. The intrusiveness of this power is however overshadowed by other powers in the Bill. Indeed, the intelligence services would, it seems, obtain ICR in bulk before they are destroyed by telecommunications companies under the bulk acquisition capability described above (although the point is not clear: apparently ICR are not currently obtained under s.94 of the TA 1994).

53. The retention power seems to be principally intended to assist the police's investigate and gather evidence of serious crime.

54. There are three problems, according to the operational case that the power to require retention of ICR is intended to address, each arising where there is a "known suspect".

(1) The first arises where the police know that a message has been sent to a criminal by an accomplice or where they know someone has, for example, participated in an online chat room for nefarious purposes. They have a suspect, but they don't know his or her identity. A message sent by a WhatsApp account, for instance, may be in a false name. Although the authorities can seek information from the webpage or messaging service provider, such efforts, for a variety of reasons, are often not fruitful. The Counter Terrorism Crime and Security Act 2015 introduced a power to require telecommunications companies to retain data necessary to resolve IP addresses to trace web usage, but if a device was sharing an IP address at the relevant time, as mobile phones in particular often do, this does not provide evidence to identify an individual. The Bill would take this further to retention of records of which webpages (up to the first slash), apps and services that a device has accessed. This is evidence which is already in principle obtainable, but in practice is not retained by telecommunications companies.

(2) The second and third problems identified by the operational case relate to a situation where a suspect is known and the police want to know which internet messaging service he or she has used in order to try and find out with whom they have been in contact. But in respect of these issues the justification may not be made out. In such a scenario an interception warrant could be obtained in respect of the suspect (which would now require JC approval) to look at contemporaneous and stored messages and associated communications data (interception, counter-intuitively, has always included looking at stored messages).

55. A key danger in enabling access to ICR is that it could allow authorities to identify suspect web-browsing patterns, perhaps in combination with other communications data, in order to identify suspect categories of person (internet records includes information about the "pattern" of communications). This is different from using such data to identify *known* (but unidentified) suspects or for identifying the contacts of <u>known</u> suspects.

56. A tightening of the legislation is warranted, in particular to ensure that the data made

available are not used beyond the operational cases articulated, i.e. in respect of known (even if unidentified) persons suspected of committing serious crimes, rather than for tracing suspicious activity in a search for suspects.

Bulk personal datasets

57. The obtaining and use of "personal datasets" by the intelligence services was unknown until March this year, when the Prime Minister gave the Interception Commissioner oversight of the practice.

58. Personal datasets are records held on individuals, ranging from driving licence records to the electoral roll. As the Bill candidly records, *"the nature of the set is such that it is likely that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service"* (cl. 150(1)(b)). But it far from clear from the Bill's documents how far this extends – medical records? Immigration histories? Tax returns? court records? – and what about privately generated data sets such as company employee records or bank account details?

59. It is proposed that obtaining and use of personal datasets will be authorised by warrant in bulk by reference to a "class" of such data sets (c. 153). These can be added to by specific personal data set warrants (cl. 154).

60. But class authorisation is inadequate. It is difficult to understand why the datasets cannot be listed expressly in any warrants so that there is clear judicial sight of what data sets are being held and used.

61. If there is to be proper democratic licence for these activities, there needs, at a minimum, to be greater visibility as to the breadth of the power, and full judicial approval.

62. Furthermore, the vague internal "arrangements" (now published) for use of such data sets leave much to be desired, e.g.:

(1) *"Individuals must only access information within a bulk personal dataset if it is necessary for the performance of one of the statutory functions of the relevant Intelligence Service"* – But everything an intelligence officer does is in furtherance of the fight against serious crime or the protection of national security so this is vacuous.

(2) *"Data containing sensitive personal data (as defined in section 2 of the DPA) may be subject to further restrictions…."*. Or, they may not

(3) *"Working practice seeks to minimise the number of results which are presented to analysts by framing queries in a proportionate way, although this varies in practice …"*. This is no protection at all.

63. Much tighter restrictions, set out in statute, should be introduced.

Equipment interference (hacking)

64. It is no doubt necessary for intelligence services to have the capability to hack into computers, telecommunications systems and smart phones, just as it is necessary for them to break and enter, burgle and bug. But such powers are extremely intrusive, potentially much more intrusive than interception of communications.

65. In theory, such capabilities would enable (amongst other things):
    - Computers and smart phones to be remotely controlled by the intelligence services to be used as a listening device or to take photographs or videos or to track individuals and their contacts.
    - The authorities to gain access to documents to stored on devices and servers that have not been communicated to others.
    - Access to communications of persons targeted at demonstrations, sports or entertainment events, or even in relation to large areas of territory (such as the alleged hack into Cisco systems' Pakistan server to obtain intelligence on jihadists in the region).
    - Exploitation of emerging technologies such as the use of smart watches that monitor heart rates and breathing patterns, the "internet of things" which connects myriad devices such as cars, household appliances, domestic security systems, etc, all of which provide new opportunities for data gathering. This possibility is intriguingly raised in the documents accompanying the Bill, no doubt to head-off any argument a few years hence that the potential breadth of this power was not anticipated.

66. The use of equipment interference powers was only publicly avowed in February 2015, when a draft Code of Practice was hurriedly introduced in attempt to shore-up the power under the ISA 1994 s.5 (property and wireless telegraphy interference warrants), the scope and use of which has always been obscure.

67. In the Bill warrants are divided between "targeted" and "bulk". Targeted warrants include thematic warrants in a similar manner to interception warrants and invoke similarly general and vague language, attracting the same concerns. The Bill would also allow warrants to be issued in relation to equipment *"in a particular location"*, which also admits of a very broad interpretation and which requires only the general location to be described, not the equipment (cl. 83, 93).

68. The authority for bulk equipment interference is novel. Section 5 of the ISA 1994 refers to warrants in relation to "specified" property or wireless telegraphy. The new Code of Practice also refers to the so-called James Bond power contained in s.7 of the ISA 1994 by which the Foreign Secretary can authorise GCHQ or MI6 to carry out otherwise unlawful acts abroad (or, by an amendment to the power, acts which are intended to have effects on apparatus situated abroad).

69. This power to do unlawful acts, which is obviously not limited to equipment interference is perhaps the most secretive of all of the intelligence services' powers,

with all queries about use of s. 7 having historically been met with an NCND response. It is under this power that a bulk authorisations for equipment interference in respect of persons abroad has hitherto been given.

70. The very broad nature of both targeted and bulk warrants has already been commented on and, given the particular intrusiveness of hacking capability, is a cause of real concern. (It is also unclear precisely what remains of s.5 of the ISA 1994, which is not set to be repealed and continues to apply to wireless telegraphy and physical property interference).

The IPT

71. The IP Bill provides an opportunity to reform the IPT.

72. The introduction of a right of appeal will bring the IPT into the civil justice system and it will no longer be a mere complaints body for surveillance and intelligence services matters. That is a good thing.

73. But once it is recognised that the IPT is an independent tribunal and part of the civil justice system, and not a mere complaints body, other changes to the legislative regime under which it operates are called for:

    (1) At present the Tribunal's rules are made by the Secretary of State (s.69(1)). It is obviously inappropriate for the IPT to determine cases pursuant to rules made by one of the parties to the complaint (as it will often be). Although the IPT does have power to dis-apply rules that are contrary to the Human Rights Act 1998, in determining this issue it gives considerable leeway and deference to the Secretary of State. Moreover, the IPT will not draft its own rules: the power to design the IPT's rules remains an extremely important power over the tribunal.

    (2) At present, the IPT cannot disclose any information or documents provided by the intelligence services or public bodies without that entity's consent. It is a fundamental constitutional principle that the courts determine whether material can be disclosed and are not dictated to by the Government (*Duncan v Camel Laird, Conway v Rimer*). It is no answer that in IPT proceedings, the Government do not have an option to concede issues as they might in other proceedings, because this option is not always open in other proceedings either legally or practically.

74. The principal limitation on the IPT at present is that individuals affected by the powers under RIPA do not know that this is the case. The recent spate of claims against the intelligence services in the IPT is attributable to the Snowden disclosures and, to some extent, recent Government avowals. That is not likely to continue. It should not be thought that it will have a prominent or energetic role in oversight in the future.

75. One restriction on the IPT's jurisdiction at present is that only the victims of

interception and surveillance can complain to it. Given that access by such individuals is limited in practice by the covert nature of such activities it is important that others should be able to complaint to the IPT, for instance, persons discovering what they believe to be unlawful action not relating to themselves, or ISPs required to implement measures which they consider to go too far.

76. Furthermore, there is no justification for the bar on legal aid being available to complainants to the IPT, particularly as it is the designated body for Human Rights Act claims against the intelligence agencies.

Judicial Commissioner's Office

77. The merger of the functions of the current commissioners is clearly desirable. However, it is important that there remains an institutional or sub-institutional separation between JCs who consider warrant applications and inspectors who engage in post-hoc investigations and monitoring.

78. It is an important part of the judicial function and vital for public confidence that persons exercising judicial functions do not receive briefings from and do not meet informally or formally with those who may come before them. The submissions and evidence presented to a judge should be limited to that which is submitted within the formal confines of the judicial or quasi-judicial process.

79. This means that it would be inappropriate for JCs to carry out the task of inspectors (or at least the same JCs). They should not be going in to the agencies and meeting with them formally or informally or visa versa. Whilst such a system has operated in relation to the Intelligence Services Commissioner hitherto, it should not be expanded under the new Act.

80. Finally, the new provisions in cl.171 of the Bill are of considerable importance but as drafted are flawed.

81. Clause 171 muddles two separate issues:

(1) A power for the chief JC – as called for by the Interception Commissioner's Office – to have a power to refer difficult cases or issues of law to the IPT.

(2) A power to disclose errors to persons affected. The Interception Commissioner currently has (set out in the Code) certain powers to inform individuals who have been subject to erroneous use of personal data. Clause 171 seems directed at bringing a similar authority into statute but sets out limitations and a requirement for IPT approval that the error is a "serious error".

82. These two issues need to be addressed separately and s.171 probably needs to be divided into two clauses each addressing one of these issues.

83. As drafted, clause 171 <u>reduces</u> the power of the oversight body by requiring IPT

approval for error reporting. That is unwarranted and is not based on any concerns about the operations of the oversight bodies. It also creates an unclear role for the IPT - which should be limited to determining whether public authorities have acted outside their powers, not advising on disclosures. And it also sets up the prospect, which is extremely undesirable, of the JC and IPT taking different positions.

84. The chief JC will be a very senior judicial figure, of greater seniority than the members of the IPT (Lord Judge was for instance the Head of the Judiciary and the boss of the judicial members of the IPT). It is not right that the JC should have to submit issues of error reporting to the IPT if he wishes to disclose these.

85. The conditions set out for disclosures are also topsy-turvy. The focus is on the seriousness of the error. But it is not the seriousness of the error but the seriousness of the consequences for national security if an error report is made to the person concerned which must be the key factor. Even a minor error should be communicated to a person if there is no reason not to do so. Whereas a serious error might not be appropriate for communication if it would tip of a suspected terrorist of an operation in respect of him.

86. The requirements that error has caused "significant prejudice or harm" to the person concerned is also, frankly, ludicrous in circumstances in which the error – which may be very serious – will have been covert. What does this mean in such a context? Does it have to be shown that the error caused some distress or financial harm to the individual concerned? Even if the person was affected by it in some way, this may not be known to the authorities or the JC. Such a condition is not only inappropriate but it would lead to the concealment of errors for which there is no national security reason for not making known to the person concerned. That is unlikely to comply with the European Convention on Human Rights.

87. The chief JC should be able to balance national security against the seriousness of the error in deciding whether to report the error to the person or organisation concerned. The JC will consider representations from the police or agencies and is perfectly capable, and it is perfectly proper, for him to make that determination himself.

88. Finally, it needs to be made clear in statute what limits there are on the disclosure power. Providing an open-ended power to limit the disclosure power by Code, as sub-clause (11)(b) currently does is certainly wrong.

89. In short, section 171 needs a complete re-think.

Conclusion

90. The Bill is an advance in terms of transparency of surveillance powers and it will bring capabilities such bulk interception, equipment interference and use of datasets out into the open (at least, in general) and subject them to a legal framework. However, numerous provisions in the Bill raise concerns, many but not all of which have been covered in this submission.

TOM HICKMAN
Barrister at Blackstone Chambers
Reader in Public Law, University College London

18 December 2015

Home Office—further supplementary written evidence (IPB0159)

The draft Investigatory Powers Bill: Further questions from the Joint Committee

Thank you for your letter of 21 December 2015, further to mine of 17 December that responded to questions raised by your Committee during the Home Office oral evidence given on 30 November. I am grateful that you could accept this supplementary material to explain the Government's position. You will note that in our submission of written evidence to your Committee on 21 December, we have provided more detailed diagrams addressing aspects of the Bill individually.

You raise the issue of bulk personal datasets and the challenge in scrutinising the proposed authorisation model with little detail of what they might contain.

The Government understands the need to offer assurance to the public and to Parliament as to the capabilities of the security and intelligence agencies in this respect. However, as you will have heard during your recent visit to Thames House, there is a need to ensure any publication of guidance, or the types of data that the agencies hold, does not jeopardise national security. There is a limit to the number of examples of BPD that can be put into the public domain without affecting national security. Further detail as to what is held, or how they are used, could incite behaviour change and reduce the utility of the information itself, or affect over time the ability of the security and intelligence agencies to carry out their statutory functions.

Nor is it possible to make public the types of dataset that currently the agencies do not hold; this may provide those that wish to do us harm greater insight as to the limits of the agencies' capabilities and thus how to avoid detection or disruption.

The national security sensitivity of publishing information about the use of BPD by the security and intelligence agencies has been recognised by the Intelligence Services Commissioner and the Intelligence and Security Committee of Parliament who provide independent oversight of this vital capability.

The Government and the existing oversight bodies have, though, provided significant information about the safeguards relating to BPD, how they would operate in the Investigatory Powers Bill, and some illustrative (albeit limited) examples. This includes:

(a) Examples of bulk personal datasets: the electoral roll, passport or firearm licence records, or a telephone directory.
(b) Example of the type of datasets: travel data.
(c) Explanation for why bulk personal datasets are useful and how they are used has been provided in the fact sheet accompanying the Bill and in the ISC Privacy and Security report.
(d) Explanation of the existing handling arrangements for BPD are provided in the security and intelligence agencies' Handling Arrangements which was published at the same time as the draft Bill's publication.

The security and intelligence agencies can only seek to obtain and examine bulk personal datasets that are necessary to their statutory purposes. In all cases, they must consider carefully the necessity and proportionality of obtaining a dataset. These safeguards are reflected in the published Handling Arrangements and the draft Investigatory Powers Bill and will be reflected in a draft statutory Code of Practice that will be published alongside the Bill in the Spring.

The draft Bill provides the 'double lock' Secretary of State and Judicial Commissioner authorisation model for the agencies' acquisition and use of BPD. This provides a robust safeguard and is consistent with the authorisation process for the most intrusive powers elsewhere in the Bill. This reflects David Anderson QC's recommendation for equivalent safeguards for BPD (recommendation 6). The authorisation model applied accords the same stringent safeguards that would be suitable for those datasets that carry the greatest sensitivity. I would therefore recommend that your Committee consider the authorisation and oversight model for BPD in this light and draw your conclusions on that basis.

The Intelligence and Security Committee of Parliament is also scrutinising the draft Bill and is able to consider highly classified material - including relating to BPD. I am copying this letter to the Chair of the ISC so he is aware of your Committee's particular interest in this area.

Urgent warrants

Separately, you and your colleagues met officials for informal briefing on the draft Bill on Tuesday 15 December. Part of the discussion covered the context in which urgent warrants might be sought. I would like to take this opportunity to reiterate the explanation in order that the Committee might be able to refer to it in its report.

It is fundamental for the security, intelligence and law enforcement agencies to be able to maintain the current levels of operational agility and pace in the future. This is vital to the agencies' ability to continue to protect national security against terrorism and other threats.

As part of this, we need to ensure that the authorisation processes which enable them to proceed with operations and investigations can happen quickly. There are often only short time frames during which the agencies can react to threats or take advantage of opportunities presented to them. In some cases this necessitates obtaining authorisations in minutes rather than hours. The urgent warrantry procedure has, of course, been in place for many years under existing legislation. In practice, a warrant is only treated as urgent if there is an immediate and limited window of opportunity to achieve the aim of the warrant. Typically the urgency provision is used in relation to a fleeting intelligence or evidence-gathering opportunity or an imminent threat to life or serious harm. Over the many years that urgent warrants have been scrutinised by the current oversight Commissioners, there has been no suggestion that the procedure has been abused.

Investigatory powers in other legislation

Finally, the Committee Clerk has passed a query from Lord Strasburger to my officials. He asked us to provide a table with details of investigatory powers that will exist outside the Investigatory Powers Bill if it is enacted as currently drafted. I trust the response, which I have attached the response to this letter, will be of use to the Committee.

I stand ready to answer any further queries you may have in the course of your scrutiny of the draft Bill.

Rt Hon John Hayes MP

POWERS AND OBLIGATIONS OUTSIDE OF THE INVESTIGATORY POWERS BILL

This table provides an overview of the powers available to public authorities that relate to the acquisition of communications and communications data in the UK, or the removal of electronic protection from communications and communications data, that would remain in other legislation if the Investigatory Powers Bill were passed in its current form. These are primarily overt, evidence gathering powers that were not directly addressed by the three independent reviews that informed the proposals in the draft Investigatory Powers Bill. The draft Bill deals with these powers to the extent that it does not prohibit their use to obtain evidence that might include communications or communications data in the ordinary course of investigations.

Powers / obligations that will remain outside of the IP bill	**Relevant statutory position**
Law enforcement and other agencies will often use search and seizure powers to authorise the examination of property. This might include, for example, mobile phones or computers. Equally, public authorities may seek court orders directing the disclosure of information, including data that is stored on a communications device. Such activity may result in the acquisition of stored communications. Within the framework of the draft Investigatory Powers Bill, such conduct may technically constitute an interception or equipment interference .The draft Bill makes clear that this is lawful.	Powers of search and seizure including: Police and Criminal Evidence Act 1984 to search or obtain material - including s.8 , s.9, s.18, s.19 and s.32 Proceeds of Crime Act 2002 to search or obtain material - including s.345 and s.352 Search powers contained in the Firearms Act 1968, Protection of Children Act 1978, Theft Act 1968 and the Misuse of Drugs Act 1971 Powers under the Customs and Excise Management Act 1979 to examine imported goods - including s.159 Powers under the Terrorism Act 2000 to examine material - Schedule 7 Stored communications may also be obtained by the police by seeking a production order. The power to seek production orders is set out in a number of different statutory provisions, many of which deal with specific types of crime such as drug trafficking or terrorism.

Officers of HM Revenue and Customs will sometimes need to examine postal items at ports in order to identify fraud. A constable, immigration officer or customs officer may do so for counter-terrorism purposes. Within the framework of the draft Investigatory Powers Bill, such conduct would technically constitute an interception. The draft Bill makes clear that the use of existing powers for this purpose is lawful.	s.159 of the Customs and Excise Management Act 1979, Schedule 7 of the Terrorism Act 2000
Prison inmates' communications will sometimes be monitored for security purposes in accordance with Prison Rules. Within the framework of the draft Investigatory Powers Bill, such conduct would technically constitute an interception. The draft Bill makes clear that the use of existing powers for this purpose is lawful.	Regulations issued under the Prisons Act 1952, the Prisons (Scotland) Act 1989 or the Prisons Act (Northern Ireland) 1953
Psychiatric hospitals will sometimes monitor patients' communications for security purposes in accordance with statutory directions. Within the framework of the draft Investigatory Powers Bill, such conduct would technically constitute an interception. The draft Bill makes clear that the use of existing powers for this purpose is lawful.	Pursuant to a direction issued under the National Health Service Act 2006 or the National Health Service (Wales) Act 2006
A small number of public authorities will sometimes use regulatory powers to secure the disclosure of information in relation to regulation of telecommunications services. Ofcom, for example, may acquire data to ensure that the rules governing use of radio spectrum are complied with. Within the framework of the draft Investigatory Powers Bill, such conduct would technically constitute the acquisition of	Relevant powers (eg, s.135 and 136 of the Communications Act 2003, s.31A of the Privacy and Electronic Communications Regulations 2001)

communications data. The draft Bill makes clear that the use of existing powers for this purpose is lawful.	
The security and intelligence agencies currently acquire information, including bulk personal datasets, under the Security Service Act 1989 and the Intelligence Services Act 1994. While the draft Investigatory Powers Bill will introduce new safeguards relating to the acquisition and use of such datasets, they will continue to be acquired under existing statutory powers. These powers cannot, though, be used to circumvent the powers to acquire communications or communications data, and the associated safeguards, in the Investigatory Powers Bill.	s. 2(2)(a) and 4(2)(a) of the Intelligence Services Act 1994 and s.2(2)(a) of the Security Service Act 1989
Law enforcement and the security and intelligence agencies will sometimes interfere with electronic equipment where the primary purpose is not to acquire communications or other private data (eg, in order to remove malicious software installed by criminals). This is not an investigatory power and is therefore not provided for under the draft Bill.	s.5 of the Intelligence Services Act 1994 and s.93 of the Police Act 1997
The Regulation of Investigatory Powers Act 2000 provides for notices to be served on persons or companies requiring them to provide protected electronic information in an intelligible form. This is typically used to require suspects in criminal investigations to provide passwords in order to unlock seized computers. This is distinct from the obligation in the draft Investigatory Powers Bill on communications service providers that are subject to technical capability notices to remove encryption.	Part 3 of the Regulation of Investigatory Powers Act 2000

13 January 2016

Home Office—supplementary written evidence (IPB0147)

INVESTIGATORY POWERS BILL: RESPONSE TO 30 NOVEMBER EVIDENCE SESSION

Further to your evidence session on 30 November with Home Office officials, I write to provide further information on two points of detail. The first relates to the judicial review test that would be applied by judicial commissioners when approving warrants under the Bill. The second relates to other legislation concerning the use of intrusive surveillance powers.

Judicial Review

The Committee asked what the Government's definition of the judicial review test was; whether the judicial commissioners would be applying the Wednesbury principle or another test; and whether it was 'reasonableness' or 'rationality'.

The principles of judicial review have been well established and applied by the courts, and the Government does not seek to change those in the present case. As the Committee will know, in general terms, judicial review proceedings are concerned with the lawfulness of a decision and not the substance of that decision or its merits. In line with the long established principles of judicial review, the role of the Judicial Commissioners will be to conduct a review in order to assess whether that decision was flawed, and not to re-make the decision.

Irrationality is just one of the grounds under which a decision can be challenged by way of judicial review. A decision is irrational if it is manifestly unreasonable or where a decision-maker has taken into account irrelevant matters or failed to consider relevant matters. The threshold is high – a decision is unreasonable if it 'is so unreasonable that no reasonable authority could ever have come to it' ('Wednesbury unreasonableness').

However, case law has made clear that judicial review is a flexible tool that allows for differing degrees of intensity of scrutiny, depending on the circumstances and the impact of the decision on the individual concerned. Lord Pannick made this point in his article in The Times dated 12 November, whilst noting judges accord the executive a margin of discretion to reflect its expertise in national security matters. I note this position was also supported by the present Commissioners that gave evidence to your Committee on 2 December. The Judicial Commissioners will hold or have held high judicial office (i.e. High Court judge or more senior) so will have significant experience of applying judicial review principles.

The Government believes the 'double lock' process for the authorisation of warrants represents a significant strengthening of current safeguards and will provide for both democratic accountability, acknowledging the expertise of the executive in considering national security matters, and independent judicial scrutiny.

I thought it would also be helpful to set out in more detail the process by which a warrant would be issued, and have attached two flow-charts to illustrate the process:

- Before a warrant application reaches a Secretary of State it would have to go through multiple layers of scrutiny both within the warrant requesting agency and the Department of State to ensure that it was lawful, necessary and proportionate. Once officials in both the warrant requesting agency and the warrant granting department are content, the application would be passed to the Secretary of State to consider. The Secretary of State would then decide whether to issue the warrant (and in doing so may seek clarification or additional information). His or her decision must include consideration of whether the warrant was necessary and proportionate.

- Once the Secretary of State (or Scottish Minister) has decided to issue a warrant, they cannot do so until it has been approved by a Judicial Commissioner. In reviewing the Secretary of State's decision, the Commissioner would have to apply the same principles as would be applied by a court on an application for judicial review. The Judicial Commissioner would have access to all of the information that has been shown to the Secretary of State and would be able to seek any clarification that he or she needed in order to reach an informed decision. If the Judicial Commissioner does not approve the Secretary of State's decision the warrant cannot be issued. The draft Bill provides an 'appeal' mechanism by which the Secretary of State may ask the Investigatory Powers Commissioner (IPC) to reconsider the decision to issue the warrant, but the IPC's decision would be final. There is no means by which a Secretary of State could overrule this decision.

- In line with the recommendations made by David Anderson QC and the Royal United Services Institute, the draft Bill makes provision for urgent cases. Such cases – for example where there is an imminent threat to life – should make up a very small proportion of the total number of warrants, as has been the case to date. The draft Bill allows such urgent warrants to be issued without prior Judicial Commissioner approval, but requires that they must be notified to, and reviewed by, a Judicial Commissioner who would have the power to cancel the warrant. The Judicial Commissioner would then have full discretion to decide what should happen to any material that has already been collected under the warrant. In the event that an urgent warrant was renewed before it expired (they would last for a maximum of five working days), then the Secretary of State's decision to renew would need to be approved by a Judicial Commissioner.

Other relevant legislation

Your Committee asked what other legislation would continue to provide for the use of covert surveillance powers by law enforcement and the security and intelligence agencies.

The draft Investigatory Powers Bill brings governs all of the powers available to the state to obtain communications and communications data. This reflects the recommendations of the three independent reviews that considered this subject.

The draft Bill incorporates relevant powers in the Regulation of Investigatory Powers Act 2000, the Data Retention and Investigatory Powers Act 2014, the Wireless Telegraphy Act

2006 and the Telecommunications Act 1984, among others. In particular, the draft Bill streamlines communications data acquisition powers so that general information gathering powers may not be used to obtain communications data from communications service providers.

Parts 1 and 2 of the draft Bill specify the circumstances in which communications or communications data may be obtained other than under the provisions in the Bill. In summary:

- Clause 5 of the Bill permits the examination of communications devices where they are lawfully in the possession of a public authority; this includes the examination of any communications stored on those devices.

- Clauses 32-38 of the Bill specify the circumstances in which interception may be authorised other than under a warrant issued under the Bill. Those instances include:

    - Where the interception is with the consent of both parties to the communication (clause 32)
    - Where the interception is undertaken by providers of postal or telecommunications services in relation to the provision of those services (clause 33)
    - Where the interception is undertaken by businesses etc. for monitoring or record-keeping purposes and subject to further requirements specified in regulations (clause 34)
    - Where the interception is undertaken by an officer of HM Revenue and Customs under s.159 of the Customs and Excise Management Act 1979 (clause 35)
    - Where the interception is undertaken by OFCOM for regulatory or enforcement purposes (clause 36)
    - Where the interception takes place in a prison in accordance with regulations made under the Prisons Act 1952, the Prisons (Scotland) Act 1989 or the Prison Act (Northern Ireland) 1953 (clause 37)
    - Where the interception takes place in a psychiatric hospital in pursuance of a direction issued under the National Health Service Act 2006 or the National Health Service (Wales) Act 2006 (clause 38)

- Clause 9 and Schedule 2 to the Bill repeal statutory powers other than those under the Bill to obtain communications data. Clause 9 preserves the ability of public authorities to secure the disclosure of information that may include communications data in relation to the regulation of telecommunications services. This includes:

    - The ability of OFCOM to acquire information, which may include communications data, under the Communications Act 2003 in order to resolve disputes about network access.
    - The ability of the Information Commissioner's Office to acquire communications data under the Privacy and Electronic Communications

Regulations 2001 to identify companies engaging in unsolicited direct marketing.

- Clause 10 of the Bill prohibits public authorities from exercising powers outside of the Bill to undertake equipment interference in order to obtain communications or private data where there is a connection to the British Islands. Equipment interference for purposes other than obtaining private data (eg, for the removal of malware implanted by criminals) may be authorised under the Police Act 1997 or the Intelligence Services Act 1994.

Nothing in the draft Bill acts to fetter the discretion of the Courts. Court orders or other judicial authorisations may therefore direct communications service providers or others to provide such data for evidential purposes.

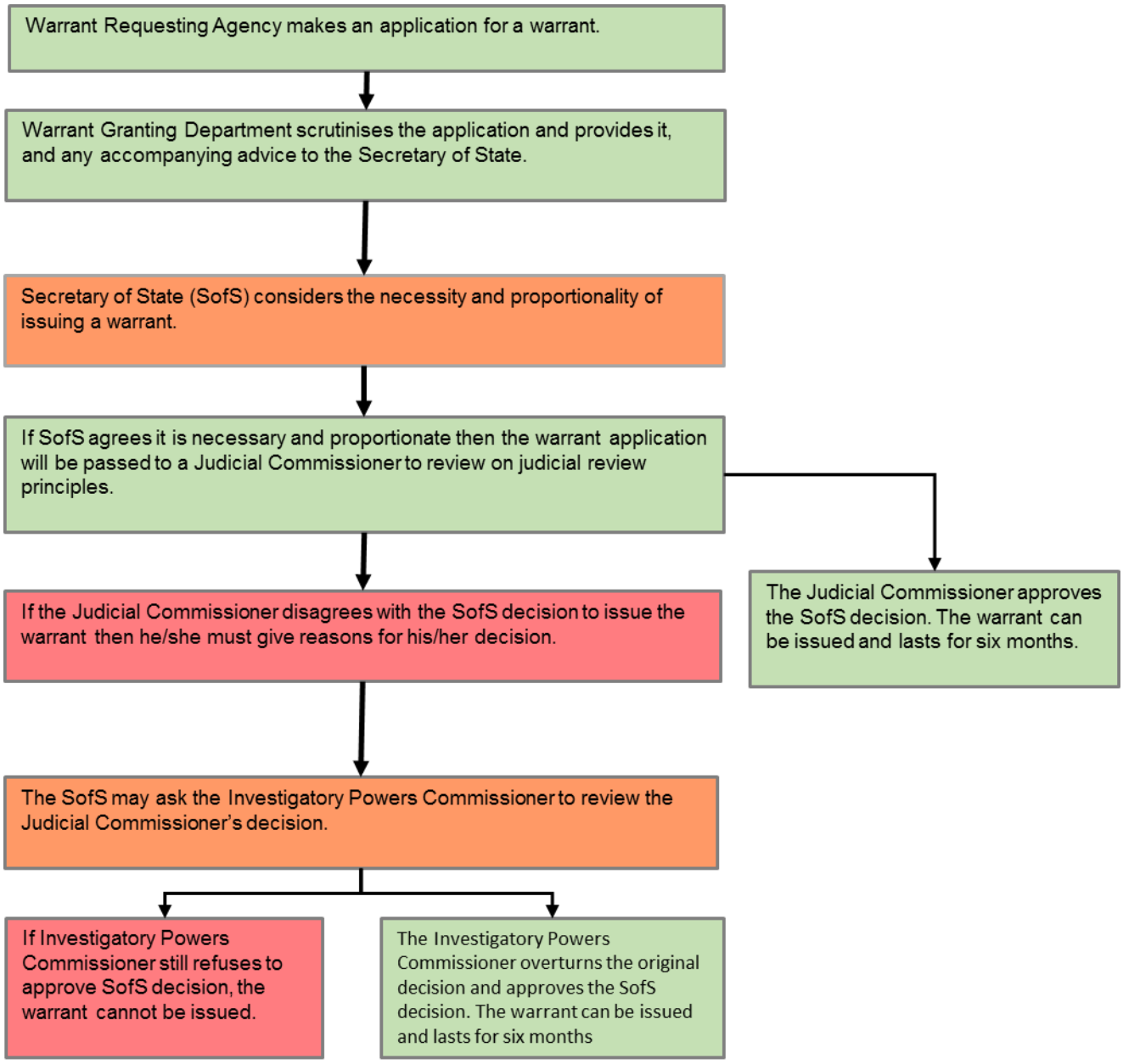
The draft Bill does not deal with the use of covert powers other than for the obtaining of communications and communications data. This reflects the scope of the reviews undertaken into investigatory powers and the Government's commitment to bring forward legislation before the sunset clause in the Data Retention and Investigatory Powers Act 2014 takes effect.

Part II of the Regulation of Investigatory Powers Act 2000 will continue to provide for directed surveillance (e.g. covertly observing or listening to someone in a public place), intrusive surveillance (e.g. the use of a covert camera or listening device in a private residence or vehicle) and covert human intelligence sources (e.g. undercover officers or informants). Equivalent provisions in Scotland are made under the Regulation of Investigatory Powers (Scotland) Act 2000.

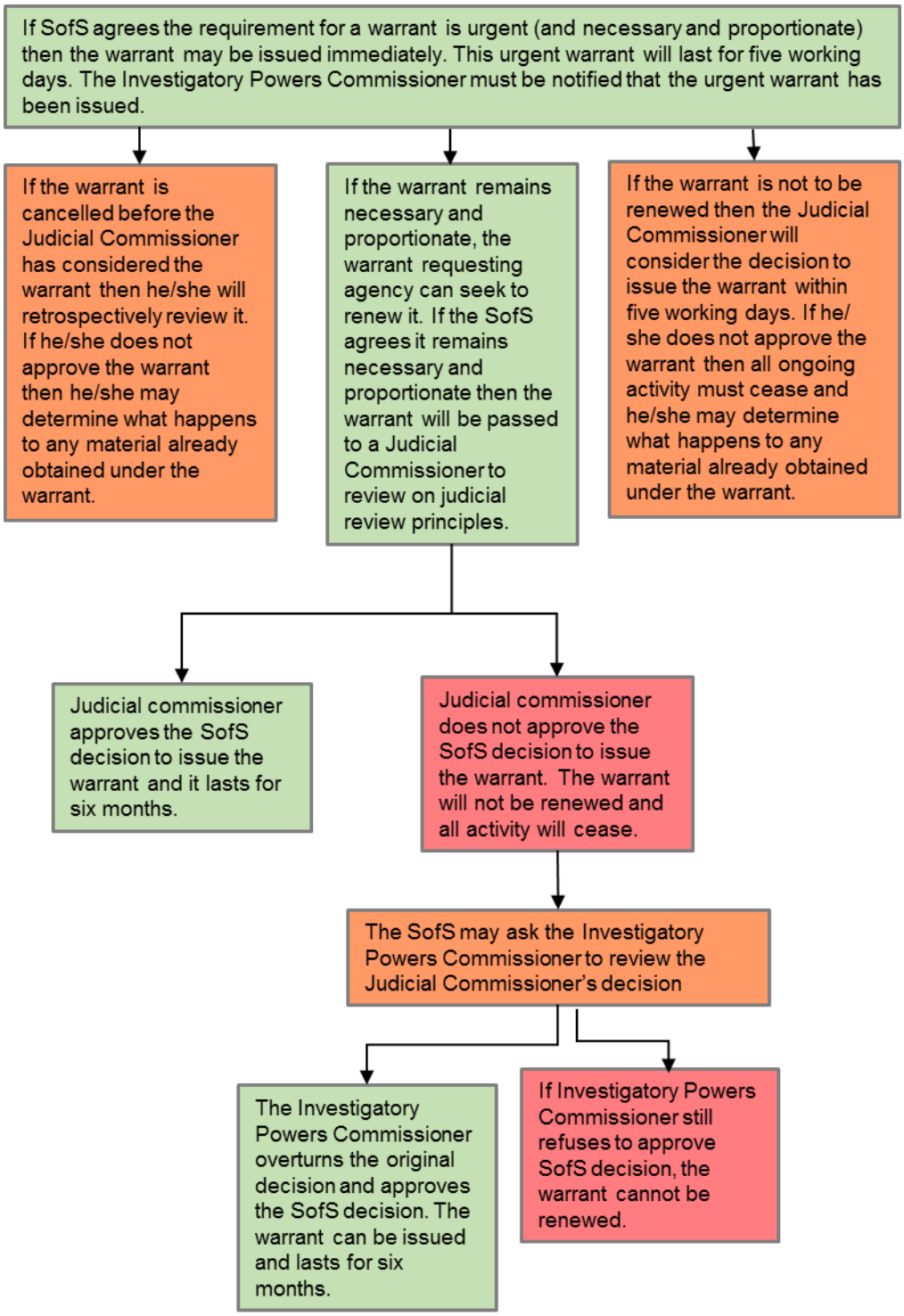
In addition, powers to interfere with property and wireless telegraphy will remain in Part III of the Police Act 1997 for law enforcement and in the Intelligence Service Act 1994 for the security and intelligence agencies.

Rt Hon John Hayes MP

Annex A: Authorisation flow-chart (non-urgent cases)



Annex B: Authorisation flow-chart (urgent cases)



Home Office—written evidence (IPB0146)

INTRODUCTION

1. This submission responds to each of the questions in the Committee's call for evidence. It stands in addition to the oral evidence provided by officials from the Home Office and the Foreign and Commonwealth Office on 30 November 2015. Further detail on areas in which the committee has signalled an interest are contained in the Annexes to this submission:

    - **Annex A:** definitions and key terms in the draft Bill
    - **Annex B:** the request filter and internet connection records
    - **Annex C:** the role of the Technical Advisory Board
    - **Annex D:** the authorisation process for each power in the draft Bill
    - **Annex E:** the modifications process.
    - **Annex F:** responses to the three independent reviews.

Are the powers sought in the Bill necessary? Has the case been made both for the new powers and for the restated and clarified existing powers? Are the powers sought legal? Are they compatible with the Human Rights Act and the European Convention on Human Rights? Is the requirement that they be exercised only when necessary and proportionate fully addressed? Are they sufficiently clear and accessible on the fact of the Bill?

2. The compatibility of the draft Bill with the UK's domestic and international human rights obligations is addressed in detail in the Human Rights memorandum published alongside the draft Bill on 4 November. The draft Bill brings together, and makes clear, the powers available to the state to obtain communications and communications data. It puts beyond doubt when those powers may be exercised and ensures that they may only be used when it is necessary and proportionate to do so. We have only brought forward one new power from the Communications Data Bill 2012, internet connection records. We have not brought forward other proposals, for example, the retention of third party data. A strong, operational case was made for internet connection records, which we have published.

Is the legal framework such that CSPs (especially those based abroad) will be persuaded to comply?

3. The Government is clear that companies providing communications services to people in the UK must comply with obligations in law to give effect to interception warrants and to provide communications data in response to lawful requests. The Data Retention and

Investigatory Powers Act 2014 (DRIPA) clarified those obligations. The draft Bill maintains the position in respect of obligations on communications service providers.

4. The draft Bill makes clear that a company only has to comply where it is reasonably practicable for it to do so and where doing so is not in conflict with the laws in the jurisdiction in which that company is based. The legislation provides a legal framework that will preserve the ability of the state to seek the assistance of communications service providers in order to uncover and disrupt threats from individuals who use their services and wish to do harm.

Are concerns around accessing journalists', legally privileged and MPs' communications suitably addressed?

5. There are additional protections that must apply when acquiring the content of the communications of those holding a profession that attracts additional sensitivity. The safeguards that must apply to sensitive professions now, are set out in the Interception of Communications Code of Practice currently before Parliament. And it is right that sensitive professions continue to have protections.

6. The draft Bill will ensure lawyers and doctors are able to do their jobs and protect the privacy of their clients and patients. But it is important that the ability of law enforcement and the security and intelligence agencies to investigate wrongdoers is not unduly fettered. The draft Bill – and the accompanying Codes of Practice – will build on provisions in current legislation to balance both.

Legal professional privilege

7. The privilege attached to the contents of communications between lawyer and client is important and must be protected. However, in the course of investigations into serious criminals and terrorists, law enforcement and the security and intelligence will sometimes need to intercept communications between suspects and their lawyers. It is important that the ability to undertake investigations is not unduly fettered.

8. The additional safeguards that apply to legally privileged communications are set out in draft codes of practice. Codes of Practice published under the Investigatory Powers Bill will build on these safeguards. They include:

- A presumption that any communications between lawyer and client or between a lawyer and another person for the purpose of litigation are privileged unless the contrary is established. Where in doubt, advice should be sought from a legal adviser.

- If acquiring communications subject to legal professional privilege is likely, this should be made clear in the warrant application and reasonable steps should be taken to minimise access to the communications subject to legal professional privilege.
- Where the intention is to acquire legally privileged communications, there must be exceptional and compelling circumstances which make this necessary.
- Before selecting for examination material intercepted under a bulk interception warrant which is likely to include result in legally privileged material, an enhanced internal authorisation procedure must be followed.
- A lawyer may only be the subject of an interception/ equipment interference operation in exceptional and compelling circumstances.
- Material identified as legally privileged should be marked as such and only retained if necessary and proportionate. A legal adviser must be consulted before material subject to legal privilege may be acted on.
- Legally privileged material must be safeguarded from becoming available to any person whose possession of it might prejudice any criminal or civil proceedings.
- In cases where legally privileged communications have been acquired and retained, this must be reported to the relevant Commissioner.

9. The Interception of Communications Code of Practice made under RIPA (the substance of which will be replicated under the new legislation) states that a lawyer will only be targeted in exceptional and compelling circumstances. This is a substantial and appropriate safeguard.

Parliamentarians

10. The draft Bill also requires the Prime Minister to be consulted before the Secretary of State can, with Judicial Commissioner approval, issue a warrant to acquire the content of an MP's communications. This will cover all warrants for targeted interception (with the exclusion of warrants authorised by Scottish Ministers) and all equipment interference that is carried out by the security and intelligence agencies. It will also include a requirement for the Prime Minister to be consulted before a targeted examination warrant can be issued to authorise the examination of a Parliamentarian's communications collected under a bulk interception or EI warrant. It will apply to MPs, members of the House of Lords, UK MEPs and members of the Scottish, Welsh and Northern Ireland Parliaments/Assemblies.

11. The requirement to consult the Prime Minister is included in the Interception of Communications and Equipment Interference Codes of Practice made under the

Regulation of Investigatory Powers Act 2000 (RIPA) and reflects current practice. These Codes are currently before Parliament.

Communications Data

12. Communications data does not attract the same privilege as the interception of communications. This position is as set out by the Interception of Communications Commissioner. However, the Government recognises that certain considerations apply in respect of journalists.

13. Issues surrounding the infringement of the right to freedom expression may arise where a request is made for the communications data of a journalist. There is a strong public interest in protecting a free press and freedom of expression in a democratic society, including the willingness of sources to provide information to journalists anonymously. Accordingly the Government recognises that requests for communications data intended to identify journalistic sources should be subject to judicial approval. Currently, the Acquisition and Disclosure of Communications Data Code of Practice requires law enforcement agencies to seek judicial authorisation before obtaining communications data to identify or confirm a journalistic source. The draft Bill builds on this by requiring the police and other public authorities to obtain approval from a judicial commissioner before making such a request.

Are the powers sought workable and clearly defined? Are the technological definitions accurate and meaningful (e.g. content versus communications data, internet connection records, etc.)?

14. The Bill includes clear, technologically neutral definitions. Codes of Practice published under the Bill will provide further detail about the application of powers in respect of particular technologies or services. Further information in respect of definitions is included at **Annex A**. Further information in respect of internet connection records and the request filter and how this works in practice is at **Annex B**.

Does the draft Bill adequately explain the types of activity that could be undertaken under these powers?

15. The draft Bill puts beyond doubt the powers available to law enforcement and the security and intelligence agencies to obtain communications and communications data. While the language of the Bill is technologically neutral, Codes of Practice will provide further detail about the application of power in respect of particular technologies or services. The draft Bill provides strong safeguards to ensure the use of the powers in the Bill is within both the letter and the spirit of the law. These safeguards include:

- The role of the Investigatory Powers Commissioner (IPC) and judicial commissioners in approving the issue of warrants and scrutinising the conduct carried out under the warrants retrospectively;
- The requirement for the IPC to report on an annual basis, and for the Prime Minister to make that report available publically. The IPC will have absolute discretion to make a report to the Prime Minister at any time, regarding any matter relating to the Commissioner's functions;
- The statutory requirement for Codes of Practice to be published with further detail and guidance on the use of powers;
- The role of the Technical Advisory Board in advising the Secretary of State whether obligations imposed on communications service providers are affordable and technically feasible. (More on the role of the TAB is at **Annex C**).

Is the wording of the powers sustainable in the light of rapidly evolving technologies and user behaviour? Overall is the Bill future-proofed as it stands?

16. The language of the draft Bill is technologically neutral in order to accommodate the rapid evolution of technology and user behaviour. Statutory Codes of Practice will make clear how the security and intelligence agencies and law enforcement exercise the powers under the Bill. Codes of Practice and secondary legislation will be kept up to date in order to reflect changes in technology and operational practices.

Are the powers sought sufficiently supervised? Is the authorisation process appropriate? Will the oversight bodies be able to adequately scrutinise their operation? What ability will Parliament and the public have to raise concerns about the use of these powers?

17. The privacy safeguards in the Bill are outlined in detail in the Privacy Impact Assessment, published alongside the draft Bill on 4 November**.**

18. The draft Bill provides a new 'double lock' authorisation procedure under which the most intrusive powers will be subject to both Secretary of State and Judicial Commissioner approval. This model provides for both democratic accountability to Parliament and independent scrutiny. Further information as to the authorisation process for the powers in the Bill is at **Annex D.** Information on what modifications can be made to warrants that have been approved by a Judicial Commissioner is at **Annex E.**

19. The IPC will have wide ranging powers, and sufficient resources, to audit, inspect and investigate any aspect of the use of investigatory powers that the Commissioner feel merits scrutiny. The Bill provides that the Commissioner must be given access to all information and documents needed to perform their functions. All those using

investigatory powers must provide every assistance necessary to the Commissioner and his or her staff.

20. Parliament will have considerable opportunity to oversee and debate the exercise of powers under the Bill. Parliament will approve secondary legislation made under the Bill, including statutory Codes of Practice that will contain further detail about the exercise of powers and their application to particular technologies. The draft Bill also requires that reports of the IPC must be laid before Parliament on an annual basis.

21. In respect of the public, the draft Bill creates a new domestic right of appeal from the Investigatory Powers Tribunal (IPT) which strengthens the regime in which an individual who believes themselves to be unlawfully surveilled may bring a case before the Investigatory Powers Tribunal. The Investigatory Powers Commissioner will also have a duty to inform members of the public who have been subjected to a serious error about the fact and their right to apply to the Investigatory Powers Tribunal for a remedy. The Commissioner will also play a wider role in assuring the public that the powers under the draft Bill are exercised appropriately.

To what extent is it necessary for (a) the security and intelligence agencies and (b) law enforcement to have access to the investigatory powers such as those contained in the Draft Investigatory Powers Bill?

22. The detailed documentation provided alongside the draft Bill makes clear the necessity of the powers in the draft Bill. This reflects and builds on the findings of three independent reviews into investigatory powers. A separate operational case for the retention of internet connection records was also published on 4 November.

Are there any additional investigatory powers that SIA and law enforcement should have that are not in the Bill?

23. The draft Bill responds to the recommendations of the three independent reviews of investigatory powers. As well as bringing together existing powers, the draft Bill responds to the detailed operational case that has been made for the retention of internet connection records. All of the other powers in the draft Bill are already provided for under current legislation. Their value and operational utility has been explored in detail by the three independent reviews to which the draft Bill responds, detail of which is contained at **Annex F**.

Are the new offences proposed in the draft Bill necessary? Are the suggested punishments appropriate?

24. In response to three independent reviews, the Bill incorporates relevant offences in existing legislation. This includes the offence of unlawful interception, currently provided for under the Regulation of Investigatory Powers Act 2000. This is an important safeguard.

25. The Bill provides for a new offence, knowingly or recklessly obtaining communications data without lawful authority. This follows a recommendation made by the Joint Committee that scrutinised the draft Communications Data Bill. As the unlawful obtaining and disclosing of communications data in such circumstances is a serious breach of a person's rights it is appropriate that doing so is an offence.

Interception

Are there sufficient operational justifications for undertaking (a) targeted and (b) bulk interception?

26. The ability to undertake targeted and bulk interception is not a new power. Targeted and bulk interception powers are currently available to nine intercepting agencies under Chapter 1 of Part 1 of RIPA 2000. Interception is a valuable intelligence gathering capability, which is vital to the work of law enforcement and the security and intelligence agencies. Its value and use was endorsed by the three independent reviews in this area.

27. With respect to bulk interception, the Intelligence and Security said: "It is essential that the Agencies can 'discover' unknown threats. This is not just about identifying individuals who are responsible for threats, it is about finding those threats in the first place. Targeted techniques only work on 'known' threats: bulk techniques (which themselves require a degree of filtering and targeting) are essential if the Agencies are to discover those threats".

Are the proposed safeguards sufficient for the secure retention of material obtained from interception?

28. The draft Interception of Communications Code of Practice, which is currently before Parliament, sets out the clear safeguards that surround the access to and retention and destruction of material obtained by interception. The Interception of Communications Commissioner oversees the retention of material obtained from interception and may make recommendations to the intercepting agencies as to the adequacy of these arrangements. As the Interception of Communications Commissioner set out in his report of March 2015, 'A typical inspection of an intercepting agency will include the following… an investigation of the procedures in place for the retention, storage and destruction of intercepted material and related communications data'.

29. Under the draft Bill, the IPC will have the function of keeping under review (including through audit, inspection and investigation) the retention of intercepted material. The draft Bill places a duty on the Secretary of State to ensure adequate safeguards are in place before authorising a warrant.

How well does the current process under Mutual Legal Assistance Treaties (MLATs) work for the acquisition of communications data? What will be the effect of the extraterritorial application of the provisions on communications data in the draft Investigatory Powers Bill?

30. Law Enforcement Agencies in the UK can generally request communications data from major overseas CSPs directly. The UK regulatory regime includes a "Single Point of Contact" model which provides consistency and expertise in terms of requests to the companies from different UK authorities. However, this is not always the case for other CSPs who will only provide communications data via the MLA route.

31. There is separate work underway to improve the quality of requests and to streamline processes under the existing UK/US Mutual Legal Assistance Treaty. But the Government does not consider that the use of MLAT will ever provide a complete, viable alternative to cooperation via direct approaches under UK legislation. This is largely because mutual legal assistance mechanisms are primarily used for the purpose of obtaining evidence. They are unsuited to intelligence gathering where operational timescales are paramount. As David Anderson said in his report: "There is little dispute that the MLAT route is currently ineffective. Principally this is because it is too slow to meet the needs of an investigation, particularly in relation to a dynamic conspiracy. For example a request to the United States might typically take nine months to produce what is sought. The MLAT route also does not address intelligence needs."

32. David Anderson recommended that extraterritorial application should continue to be asserted in relation to UK warrants and authorisations.

33. The effect of the extraterritorial application of the provisions in the Bill therefore, is to maintain the continued access of law enforcement and the security and intelligence agencies to communications data, provided for in existing legislation and clarified in DRIPA.

<u>Communications Data</u>

Are the definitions of content and communications data (including the distinction between 'entities' and 'events') sufficiently clear and practical for the purposes of accessing such data?

34. The draft Bill needs to apply across a range of technologies in a highly complex and fast moving area. It needs to apply equally to the technologies of the future as it does today. Accordingly the language of the legislation has to be technology neutral in order to achieve this aim.

35. The definitions in the draft Bill are intended to strike the appropriate balance between clarity, practicality and technological neutrality; the scope of the definitions is subject to clear and appropriate limits. The definitions are subject to on-going consultation with communication service providers and other stakeholders. The definitions of communications data consolidate the existing three categories of communications data under RIPA into two. In a response to the recommendation from David Anderson, the draft Bill introduces a new definition of 'content' and makes clear the strict safeguards that apply to this most sensitive type of data (Further detail as to how the draft Bill responds to the recommendations of the three independent reviews is at **Annex F**). Codes of Practice issued under the Bill will complement the explanatory documents that have been published by the Home Office providing examples of how the definitions operate in practice. Further information on definitions is provided at **Annex D.**

Does the draft Bill allow the appropriate organisations, and people within those organisations, access to communications data?

36. The Government considers this to be the case. Communications data has always been essential to a wide range of public authorities. For example, it helps the Financial Conduct Authority to investigate insider trading and the Maritime and Coastguard Agency locate people lost at sea.

37. This is the first time all these authorities have been included on the face of primary legislation. Under RIPA they are set out in secondary legislation.

38. David Anderson said that "Public authorities with relevant criminal enforcement powers should in principle be able to acquire communications data. It should not be assumed that the public interest is served by reducing the number of bodies with such powers, unless there are bodies which have no use for them."

39. In response to that conclusion, all these authorities were required to make the case that they need powers. Those cases were carefully considered, including the seniority of authorising officers, and the draft Bill makes some changes to the bodies that have access to communications data.

40. In total, forty-seven categories of public authority, making up between 500 and 600 public authorities, of which over 400 are local authorities, can acquire communications

data. Powers have been removed from the Prudential Regulation Authority because their case was not considered to be sufficiently strong. The Scottish ambulance services considered that they no longer required powers, so the draft Bill removes them. The Ministry of Defence has been added to the list of authorities: this rectifies a long running inconsistency that that Ministry of Defence has been able to intercept communications but not acquire communications data.

41. The Food Standards Agency has also been added to the list of public authorities; this reflects the fact that, following the horsemeat scandal, the Government set up a food crime unit to tackle such crimes in the future. When investigating food crimes it is crucial to be able to demonstrate links between the various parts of the supply chains, this is something communications data is essential for.

42. Detail of the safeguard provided by the request filter, which, when used, will limit the flow of communications data to public authorities from a service provider to that which is strictly necessary, is at **Annex B.** The request filter will be established and maintained by the Secretary of State, effectively in the Home Office (although there is provision to transfer its functions to another public authority), sitting between a CSP and public authorities.

Are there sufficient operational justifications for accessing communications data in bulk?

43. Where a security and intelligence agency has only a fragment of intelligence about a threat or an individual, communications data obtained in bulk may be the only way of identifying a subject of interest.

44. Access to large volumes of data is essential to enable the identification of communications data that relates to subjects of interest and to subsequently piece together the links between them. Carefully directed searches of large volumes of data also allow the agencies to identify patterns of activity that significantly narrows down the areas for investigation and allow them to prioritise intelligence leads.

45. Identifying the links between individuals or groups can also help the agencies to direct where they might request a warrant for more intrusive acquisition of data, such as interception. It allows agencies to search for traces of activity by previously unknown subjects of interest who surface in the course of an investigation in order to identify them. Access to domestic bulk communications data has enabled MI5 to thwart a number of attacks here in the UK. In 2010, when a group of terrorists were plotting attacks in the UK, including on the London Stock Exchange, the use of bulk communications data played a key role in MI5's investigation. It allowed investigators to

uncover the terrorist network and to understand their plans. This led to the disruption of their activities and successful convictions against all of the group's members.

46. David Anderson said in his report: "Together with other information, bulk data allows a more complete intelligence picture to be drawn. Without it, it may not be possible to discover new threats and follow a lead to a point of closely targeted intervention".

Is the authorisation process for accessing communications data appropriate?

47. Authorisations will have to set out why accessing the communications data in question is necessary in a specific investigation for a particular statutory purpose, and how it is proportionate to what is sought to be achieved. The authorisation process for communications data can be found at **Annex D**.

Targeted acquisition of communications data

48. Communications data can only be accessed when it is necessary and proportionate to do so. All authorisations need to seek the advice of the Single Point of Contact (SPoC). The SPoC's role is to ensure effective co-operation between law enforcement and the security and intelligence agencies and communications service providers and to facilitate lawful acquisition of communications data. They also play a quality control role, ensuring that applications meet the required standards.

49. Once it has gone through the SPoC, the authorisation will be signed off by a Designated Person at a rank approved by Parliament, who is independent of the investigation for which the communications data is needed. The requirement for an independent designated person may be waived in exceptional circumstances - e.g. where in specific cases the requirement for operational independence would undermine national security.

50. The Bill will provide a power that can be used to ensure that public authorities which access communications data infrequently (for example the Food Standards Agency or Gambling Commission) may be required to go through a shared SPoC (for example, by making use of the SPoC function within the National Anti-Fraud Network, as recommended by David Anderson). All local authorities must go through NAFN when making their requests. This will help to ensure that all applications are consistent and of sufficient quality.

51. The Joint Committee that scrutinised the draft Communications Data Bill in 2012 upheld the current SPoC process for authorisation of communications data.

52. Independent oversight of CD powers will be provided by the IPC. As with its predecessor, the Interception of Communications Commissioner's Office, the Commission will audit public authorities' compliance with CD acquisition powers and produce reports that will be made publicly available on an annual basis.

53. We will provide in the Code of Practice that public authorities must seek the advice of a judicial commissioner in relation to requests for communications data that would be novel or contentious.

Acquisition of bulk communications data

54. Bulk acquisition warrants for communications data will be issued by the Secretary of State. The Secretary of state will not be able to issue such a warrant without the decision to do so being approved by a Judicial Commissioner. This will provide a new "double-lock" authorisation procedure.

55. A bulk acquisition warrant will need to set out specified "Operational Purposes" for which any of the data that has been collected can be examined, i.e. looked at. Those specific purposes will be approved by a Secretary of State and a Judicial Commissioner and might include, for example: "attack planning by Daesh (ISIL) in Syria against the UK". No data may be examined except for those purposes.

56. Only the security and intelligence agencies will be able to apply for a bulk CD acquisition warrant and only in relation to three statutory purposes: in the interests of national security, for the prevention and detection of serious crime and in the interest of the economic well-being of the UK, where there is also a direct link to national security. National security must always be one of the statutory purposes for which a bulk interception warrant is authorised.

57. Bulk acquisition warrants must be served on a communications service provider. The power cannot be used to acquire communications data from a telecommunication system. A maintenance of technical capability notice may be issued alongside a bulk CD acquisition warrant. This would allow a communications service provider to seek a review of the technical aspects of a warrant without being able to appeal the warrant itself. Existing handling arrangement will be incorporated into a new code of practice.

Data retention

Do the proposed authorisation regime and safeguards for bulk data retention meet the requirements set out in the CJEU Digital Rights Ireland and the Court of Appeal Davis judgments?

58. The Court of Appeal has recently decided to refer questions about the interpretation of the Digital Rights Ireland judgment to the European Court of Justice. The existing regime, which contains enhanced safeguards in response to that Judgment, was approved by Parliament in 2014 and is replicated in the draft Bill.

Is accessing Internet Connection Records essential for the purposes of IP Resolution and identifying persons of interest? Are there alternative mechanisms? Are the proposed safeguards on accessing Internet Connection Records data appropriate?

59. David Anderson QC considered the issue of internet connection record retention and made clear in his report that a strong operational case needed to be made to include these provisions in the Bill. That operational case has now been made and is published on gov.uk. It made clear the utility of ICRs for resolving IP addresses and identifying persons of interest.

60. Different countries have different regimes and laws. That other countries do not require the retention of ICRs does not mean those powers are not required. Where those countries have not enabled the retention of and access to this data their law enforcement agencies simply cannot investigate some types of crime, or they may have to use alternative means to get the evidence which may be even more intrusive. Through accessing ICRs, law enforcement agencies may be able to discount any of those more intrusive options as disproportionate.

61. In outlining the purposes for which law enforcement said they needed accessing to weblogs, David Anderson said: “I have no doubt that retained records of user interaction with the internet (whether or not via web logs) would be useful for each of those purposes”. There is a strong operational case behind all three purposes for which internet connection records can be obtained.

62. The Government believes the proposed safeguards are appropriate: The acquisition of ICRs is subject to the same rigorous safeguards as any other CD request. This data can only be accessed for limited and specified purposes. Local authorities are prohibited from accessing ICRs for any purpose. Law enforcement and the agencies can only access CD where it is necessary and proportionate to do so in relation to a specific investigation. Further detail on how ICRs will work in practice as at **Annex B**.

Are the requirements placed on service providers necessary and feasible?

63. The only new power in the Bill – the requirement for communications service providers to retain internet connection records when given a notice by the Secretary of State – has been the subject of extensive and on-going consultation with industry. In light of these

discussions, the Government is clear that all of the requirements placed on service providers are necessary and feasible.

64. The draft Bill includes clear provisions for communications service providers to appeal, should a company consider that the obligation placed on them would not be technically feasible or would incur unreasonable costs. In those cases a service provider can seek a review of the obligation being imposed by the Secretary of State. In considering the review, the Secretary of State must take account of the views of the Technical Advisory Board – which comprises experts from industry and Government – and the IPC. Both of those bodies must seek evidence from the company concerned before putting advice to the Secretary of State. Further information about the composition and role of the Technical Advisory Board is at **Annex C**.

Equipment Interference

Should the SIA have access to powers to (a) undertake targeted and (b) bulk equipment interference? Should law enforcement also have access to such powers?

65. The draft Bill does not provide for new powers for the security and intelligence agencies or law enforcement in respect of equipment interference (EI). Existing legislation provides the security and intelligence agencies with the power to authorise and conduct EI, under Section 5 of the Intelligence Services Act 1994. Historically, the security and intelligence agencies have largely been able to find and follow their targets through the use of interception. This capability remains critical, but technological advances and the spread of ubiquitous encryption – wrapping information in an impenetrable blanket from sender to receiver – is resulting in an increasing number of circumstances where interception is simply not possible or effective.

66. Where the targets' devices are known, the agencies will carry out EI against those specific pieces of equipment. This approach constitutes the vast majority of EI operations and falls within the targeted regime. With the information available from interception in particular continuing to decline, there are likely to be instances in the future where it is not possible to describe the devices of interest with the necessary high degree of specificity. In such instances, the only way in which these devices can be found and identified is through what is known as 'target discovery' – i.e. using EI to acquire data from a less strictly defined set of devices, and then filtering the results of this initial EI activity.

67. For example, the security and intelligence agencies may know of a terrorist group planning an attack against the West in a given overseas region, but there may be no additional information available which sufficiently identifies the specific devices used by the terrorist group. The security and intelligence agencies may therefore aim to interfere

with all devices within a limited geographical area within which the terrorist groups are known to be operating. This type of EI operation would fall within the provisions providing for the issue of bulk EI warrants, as the category of devices authorised by the warrant to be interfered with is less focussed, and is almost certain to include devices that will not be of intelligence interest. Under the Bill, this sort of 'bulk' EI operation would be for the purpose of obtaining overseas-related communications, private information or equipment data, and would be used to identify the most serious threats in circumstances where no other methods of detection are available.

68. Currently, equipment interference is authorised by law enforcement agencies under section 93 of the Police Act 1997, which provides for interference with property and is used regularly in a wide range of serious crime investigations. The draft Bill requires that law enforcement in future seek equipment interference warrants to provide for such activity where it is intended to obtain communications or other private data. This will mean that all future use of these techniques must be approved by a Judicial Commissioner. Under the draft Bill, law enforcement may only conduct activity on a targeted basis. Equipment interference is not a single technique, but a wide range of different techniques. Some of these are very advanced, requiring highly specialist skills and equipment for very complex operations. Other techniques are relatively simple but nevertheless yield vital intelligence and evidence.

69. It is right that mainstream policing, who are at the forefront of serious crime investigations, have the less intrusive equipment interference techniques available to support their investigations. But it is also important that the use of more specialised techniques is restricted to specialist teams – as is the case across policing now – with the most sensitive capabilities delivered by the National Crime Agency on behalf of wider policing. Law enforcement use of existing property interference powers is addressed in the Covert Surveillance and Property Interference Code of Practice published under RIPA. The draft Bill will require that a statutory Code of Practice for equipment interference is published and this will set out the restrictions on the use of equipment interference by police forces.

Are the authorisation processes for such equipment interference activities appropriate?

70. Warrants for law enforcement use of equipment interference will be issued by a law enforcement chief and approved by an independent Judicial Commissioner. An authorisation can be applied for only for the prevention and detection of serious crime. Warrants for the use of equipment interference by the armed forces will be issued by a Secretary of State and approved by an independent Judicial Commissioner. A warrant can be applied for in the interests of national security. Warrants for the use of equipment interference by the security and intelligence agencies will be issued by a Secretary of State and approved by an independent Judicial Commissioner. A warrant can be applied for in the interests of national security, preventing and detecting serious

crime, and in the interests of economic well-being (where they are also relevant to the interests of national security).

71. Further detail on the equipment interference authorisation process is at **Annex D**.

Are the safeguards for such activities sufficient?

72. The Investigatory Powers Bill provides for a new, warranted model of authorisation for equipment interference with Codes of Practice providing detailed requirements for the acquisition, retention, destruction, storage and access to material obtained by equipment interference, overseen by the IPC.

Targeted Equipment Interference.

73. Law enforcement will be limited to equipment interference for the prevention and detection of serious crime, and the Code of Practice will make clear that the use of the more specialised techniques is restricted to specialist teams – as is the case across policing now – with the most specialist capabilities delivered by the National Crime Agency on behalf of wider policing. A Chief Constable or equivalent must issue a warrant for equipment interference, and a judicial commissioner must approve a warrant before it can come into force. This is a new safeguard.

74. A warrant for the security and intelligence agencies to conduct equipment interference must be issued by the Secretary of State and approved by a judicial commissioner. This is a new safeguard. Warrants may only be issued by a Secretary of State where he or she is personally satisfied that the activity would be both necessary and proportionate. A warrant can be applied for in the interests of national security, preventing and detecting serious crime, and in the interests of economic well-being in the UK (where they are also relevant to the interests of national security). Equipment interference warrants will last for six months. Urgent equipment interference warrants will last for a maximum of five days unless renewed and approved by a Judicial Commissioner. The Bill will limit the use of EI to the same statutory purposes as interception.

75. A statutory Code of Practice will set out the handling, retention, destruction and audit arrangements for the data obtained by targeted equipment interference that applies to law enforcement, armed forces and security and intelligence agencies.

Bulk Equipment Interference

76. Warrants for bulk equipment interference may only be issued by a Secretary of State where he or she is personally satisfied that the activity would be both necessary and proportionate. A Judicial Commissioner must approve the warrant before it comes into

force. This is a new safeguard. Warrants for bulk equipment interference will last up to 6 months. The Secretary of State can renew the warrant if it continues to be necessary and proportionate and the Judicial Commissioner approves. Bulk equipment interference will be limited to use on overseas devices, and would be used to identify the most serious threats in circumstances where no other methods of detection are available. The bulk equipment interference regime also imposes additional access controls before any material collected can be selected for examination. These controls include the need to establish that any examination of the data acquired by the operation is only carried out for one of the specified operational purposes approved by the Secretary of State and Judicial Commissioner and that the examination is necessary and proportionate. Further, an additional warrant is required if an analyst wants to search for the content of communications of a person known to be within the British Islands.

77. A statutory Code of Practice will set out the handling, retention, destruction and audit arrangements for the data obtained by bulk equipment interference.

78. The intelligence agencies and law enforcement's use of equipment interference does not provide 'backdoors' for criminals to exploit. The Government is committed to internet security and makes considerable effort in helping to make all of us safer online. To leave targets open to exploitation by others would increase the risk that their privacy would be unnecessarily intruded upon.

79. The safeguards that apply to equipment interference are equivalent to those for interception – the highest threshold provided for in acquisition of communications.

Bulk Personal Datasets

Is the use of bulk personal datasets by the security and intelligence agencies appropriate? Are the safeguards sufficient for the retention and access of potentially highly sensitive data?

80. The task of defending the UK's interests and protecting its citizens in a digital age is becoming increasingly complicated and challenging. The use of bulk personal datasets (BPDs) by the intelligence agencies is a critical part of their response to that challenge. The Intelligence and Security Committee said in its Privacy and Security report that BPDs are an "increasingly important investigative tool for the Agencies" and that "the Committee has examined the lists of Bulk Personal Datasets that the Agencies can access: we consider that they are relevant to national security investigations". The Government provided a summary of the use of BPDs in the associated factsheet and impact assessment published on 4 November.

81. The Intelligence Services Commissioner currently provides independent, external oversight on a statutory basis of the acquisition, use, retention, disclosure, storage and deletion of BPDs. The Commissioner has full access to the security and intelligence agencies' holdings. In his 2014 report, the Commissioner emphasised that "the case for holding BPD has been established in each service' and that 'the agencies all have strict procedures in place in relation to handling, retention and deletion." The IP Bill continues, and strengthens, this form of oversight: it places a specific statutory duty on the Investigatory Powers Commissioner to keep under review the acquisition, retention, use or disclosure of BPDs.

82. The use of BPDs is not new, and the IP Bill does not provide new powers for acquiring BPDs. Rather, it provides robust and transparent safeguards around BPDs, including a requirement for warrants to authorise the obtaining, retention and examination of BPDs. These safeguards are comparable to those provided for in relation to other powers under the Bill. They include introducing a "double-lock" so that the issue of security and intelligence agencies' warrants will in future be subject to approval by both a Secretary of State and a Judicial Commissioner. The Secretary of State can only issue warrants related to BPDs if he or she considers that it is necessary and proportionate to do so, and the Judicial Commissioner must approve that decision. The Government considers these new and stronger safeguards to be appropriate.

83. The acquisition and use of BPDs is – and will continue to be – tightly controlled, and strict handling arrangements, processes and safeguards regulate all forms of access to the datasets. The intelligence agencies must ensure that appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction or, or damage to, personal data.

84. The Intelligence Services Commissioner's oversight of BPDs includes the misuse of data and how this is prevented. In his last annual report, he said "I review the possible misuse of BPD and how this is prevented". He reported that "the agencies take any deliberate misuse of the system seriously and sanctions include dismissal, revocation of security clearance and possible criminal prosecution' and noted that 'Unacceptable uses are… few in number."

Oversight

What are the advantages and disadvantages of the proposed creation of a single Judicial Commissioner to oversee the use of investigatory powers?

85. The Government set out the benefits of the proposed change from the current tripartite oversight model, in the oversight impact assessment published on 4 November. This approach, which reflects David Anderson's recommendations in particular, will simplify the current system and should increase public and Parliamentary understanding of oversight. The draft Bill seeks to ensure that public and Parliamentary trust and confidence in the rigour of Commissioner oversight is strong. The current oversight framework is strong and holds the users of investigatory powers to account, but it is fragmented. Having one senior independent judicial figure, the IPC, who is ultimately responsible will help ensure consistent standards between the users of investigatory powers and allow best practise to be shared. It will also enable the one oversight body to have visibility of how intrusive powers are being used across a single operation or investigation (regardless of whether it was law enforcement agencies or intelligence agencies that were using the power).

Would the proposed Judicial Commissioner have sufficient powers, resources and independence to perform its role satisfactorily?

86. The IPC will have the ability to scrutinise any use of investigatory powers by a public authority. As has been made clear in the oral evidence given to the Committee by the current Commissioners, the Judicial Commissioner will be a senior Judge, used to independent decision making. The Bill provides that the Secretary of State must equip the Judicial Commissioners with such staff, accommodation, equipment and facilities as the Secretary of State considers necessary for the carrying out of the Commissioner's functions. The Secretary of State must consult the IPC on this. The oversight impact assessment contained an estimate of the financial resource that will be available to the Commissioner. This is an increase compared to the present financial resource available. The Commissioner will have access to legal, technical and communications support in addition to a budget to purchase whatever other advice and expertise that they feel is necessary.

Are the appointment and accountability arrangements for Judicial Commissioners appropriate?

87. The Prime Minister will be responsible for appointing the Investigatory Powers Commissioner. The Prime Minister will do so after consultation with the Lord Chief Justice and the Scottish Government and Northern Ireland Executive. The Prime Minister will also appoint Judicial Commissioners but will only do so after consultation with the Investigatory Powers Commissioner.

Are the new arrangements for the Investigatory Powers Tribunal including the possibility of appeal adequate or are further changes necessary?

88. The Tribunal will be strengthened through the introduction of a new domestic route of appeal. The Government does not consider that further changes to the constitution, role or function of the Tribunal are necessary.

Annex A: Terminology and Definitions

Background

1. The Investigatory Powers Bill is drafted in such a way that the definitions set out at Part 9, Chapter 2 are technology-neutral and flexible in order that, should user behaviour and technology change, they will still apply. Detailed Codes of Practice for the powers in the draft Bill will provide further information as to how public authorities can exercise powers. It is the Government's intention to publish draft Codes of Practice when the draft Bill is introduced.

2. It is generally agreed that different types of data may give rise to different levels of intrusion. In particular, the inherent differences between communications data and content justify differences in the legal framework governing the acquisition and examination of these data. In his report, David Anderson QC recommended that the definitions of content and of communications data, and any subdivisions, should be reviewed. In response to this recommendation, the Investigatory Powers Bill creates clearer, technologically neutral categories of data.

3. The Regulation of Investigatory Powers Act 2000 (RIPA) defined data relating to communications and telecommunication systems and services, e.g. communications data that was available to a communications service provider or that was intercepted during the course of transmission by means of a telecommunication system. Under RIPA, communications data was divided into three sub categories: traffic data, service use information and subscriber information. Any data falling outside of these definitions was described as content.

4. The draft Investigatory Powers Bill differs from RIPA in that it brings together powers and obligations in several other laws, including the Data Retention and Investigatory Powers Act 2014 and the Telecommunications Act 1984. It also provides for the acquisition of data via equipment interference (EI) warrants, as well as interception warrants and communications data authorisations. The definitions must therefore cater for stored and static data held on devices that has never been communicated, as well as data that has been communicated.

5. Technology has developed at a radical pace since RIPA was drafted. The variety and type of data has changed and will change more in the future. In order to make this

legislation last, the definitions in the draft Bill must be technology neutral and must cover all possible data types. This note provides further information on the key terms in the draft Bill.

Communications data

6. Communications data does not include the content of a communication.

7. This data can be held by a CSP or can be available from a communications network. The data can identify a person or device on the network, ensure that a communication reaches its intended destination, describe how the communications can move across the network, or even how a person has been using a service available over that network. It also includes data held by CSPs about the architecture of a telecommunications system which is not about a specific person.

8. Communications data is divided into entity data and events data:

- Entity data: this data is about entities or links between entities which identifies or describes the entity. An entity is a person or thing, and includes individuals, groups and objects such as mobile phones etc.

- Events data: this data identifies or describes events by means of a telecommunication system; a communication event comprises one or more entities engaging in an activity as a specific point in time.

9. The definitions of entity data and events data are relevant in the context of the authorisation regime for obtaining communications data in Part 3 of the draft Bill.

Related Communications Data and Equipment Data

10. Related communications data and equipment data are non-content data obtained under interception warrants and equipment interference warrants respectively. These data are wider than the categories of data that can be obtained by means of a communications data authorisation (i.e. they include but are not limited to communications data).

11. Distinguishing these data from content means that appropriate safeguards and handling safeguards can be consistently applied: for example, the Secretary of State may specify that a bulk interception warrant should authorise the obtaining of related communications data only, and that any content acquired under that warrant should not be made available for subsequent examination.

12. The definitions of related communications data and equipment data in the draft Bill are materially the same. This ensures that data are classified in the same way regardless of whether they are held on a device or are obtained in transmission. The data equivalence principle provides for consistency between the static/stored data available on a device and data obtained from communications in the course of transmission.

13. Both related communications data and equipment data can include communications data and any systems data which enables or otherwise facilitates the functioning of any system or service provided by the system. Systems data is not content. It is also possible for certain structured data types to be extracted from the content of a communication or an item of private information under a warrant. All related communications data and equipment data so obtained will be subject to the handling safeguards set out in the draft Bill.

14. These definitions are a balance between meeting the operational requirements of the intelligence agencies to protect the public from terrorists and serious criminals, while protecting the most private information with stringent safeguards. The definitions are also sufficiently robust and technology neutral to cater for new technologies that come online as the internet adapts and changes.

Content

15. The draft Bill provides extra safeguards for the content of a communication or other item of private information. In the draft Bill, the content of a communication or item of private information is defined as any data which reveals anything of what might reasonably be expected to be the meaning of the communication. It disregards any meaning arising from the fact of the communication or any data relating to the transmission of the communication.

Equipment

16. Clause 105 sets out that 'equipment', as referred to throughout Part 5 and Part 6 chapter 3, means equipment producing electromagnetic, acoustic or other emissions or any device capable of being used in connection with such equipment.

17. In practice this will typically include traditional computers or computer-like devices such as tablets, smart phones, cables, wires and storage devices which are capable of storing or providing meaningful, useful information.

18. The definition of equipment does not permit interference with a wider range of devices or data than could currently be authorised under the property interference powers in the Police Act 1997 or the Intelligence Services Act 1994. However, the draft Bill requires that where the intention is to obtain communications or other private information by interference with equipment where there is a link to the UK, the authorisation regime in the draft Bill (and the enhanced safeguards that apply to it) should be used.

Telecommunications operator

19. Clause 193 sets out a number of different definitions which apply in respect of the different powers contained in the draft Bill: "telecommunications operator" which means a person who offers or provides a telecommunications service to persons in the UK, or controls or provides a telecommunications system which is in the UK, or controlled from the UK. This builds on and brings clarity to the various relevant definitions in the Regulation of Investigatory Powers Act 2000, the Data Retention and Investigatory Powers Act 2014 and the Telecommunications Act 1984. The obligations in relation to targeted and bulk communications data acquisition and communications data retention apply to telecommunications operators. Similarly, the obligation to take steps to give effect to a targeted or bulk interception or equipment interference warrant applies to a telecommunications operator. The draft Bill includes further key terms:

- "telecommunications service" which means any service that consists in the provision of access to, and facilities for making use of any telecommunication system. Examples of this would be email services, fixed phone lines or mobile phones. This is differentiated from a "public" telecommunications service in that it does not have to be provided to the UK public or a substantial section of the public in the UK. The draft Bill (in clause 193(11)) provides further detail on the definition of a "telecommunication service" making clear that it includes a service which includes the creation, management or storage of communications that are or may be transmitted thus confirming that the definition includes all "over the top" services such as cloud storage.

- "telecommunication system" which means a system that exists for the purpose of transmitting communications by any means involving the use of electrical or electromagnetic energy. This includes any infrastructure services such as the public switch telephone network. This is distinct from a public telecommunication system because the infrastructure can be wholly or partly in the UK or elsewhere – therefore infrastructure could all be located outside the UK.

- "public telecommunications service" which means any 'telecommunication service' which is offered or provided to the public or a substantial section of the public in the UK. An example might be Sky email service, BT fixed line or EE mobile phone.

- "public telecommunications system" which means any parts of a telecommunications system by which a public telecommunication service is provided which are located in the United Kingdom. An example of this might be BT infrastructure.

- "private telecommunication service" which means any telecommunication service which is not a public system, but is attached (directly or indirectly) to a public telecommunication system and which includes apparatus which is located in the United Kingdom and used for making the attachment to the public telecommunication system. An example of this would be a large company internal

phone network (providing it has a way of connecting to the public telecommunications network).

Content and communications data

20. The table below provides examples as to what, in relation to a range of existing communications technologies, would fall within the definition of 'content' and 'communications data' in the context of Parts 3 and 4 of the draft Bill. In order to ensure the draft Bill can stand the test of time, it would not be appropriate to include this level of detail on the face of the legislation.

Communications data			Content
Postal			
• Name of a customer of a postal product • Address of a customer of a postal product • Phone number of a customer of a postal product • Email address linked to a customer's account of a postal product	• Any redirections in place on a customer's account • Account details used to pay for the service • The address on a letter or parcel in the postal system	• Any replacement address put on a letter or parcel to facilitate re-direction • Billing data for sending mail (e.g. corporate account)	• The content of a letter or parcel NB for a postcard the content would be the message on the postcard and picture on the front. The address and other information added to facilitate delivery of the package would be communications data.
Mobile Telephony including SMS, MMS, EMS			
• Cell mast name • Cell mast locations • Cell mast sector • Network maps • 2G/3G/4G coverage maps • Name/address of a customer	• Email address linked to a customer's account • Device identifiers linked to a customer's account –e.g. IMSI, IMEI, Mac Address • Account details used to pay for the service • Dialled phone number • Phone number of a customer	• Dialling phone number • Time/date/location a phone call was made • Device identifiers linked to a communication • Billing data • A handshake between a phone and a cell mast so the network knows where to route a call	• The audio of a phone call • The body of a text message • An image sent as an MMS
Internet access NB – this may additionally include information in relation to internet applications (below) where held by the internet access provider for business purposes			

Broadband

- Routing information
- Name of a customer
- Address of a customer
- Phone number of a customer
- Device identifiers linked to a customer's account –e.g. IMSI, IMEI, MAC Address
- Email address linked to a customer's account
- Account details used to pay for the service
- User name
- Password
- Billing data
- RADIUS logs (IP session start/stop)
- Destination IP address and port number
- The domain url (this is the part such as bbc.co.uk)**
- Server Names indicator**
- Public source IP address and port number
- Time/date/location of an internet communication

Public Wi-fi

Instead of the location/address of the broadband router the following data may additionally be captured:

- Wi-fi access point name
- Wi-fi access point address
- Wi-fi access point device identifiers e.g. MAC address
- Coverage maps

NB – What may appear as a single wi-fi access session to a customer may actually constitute multiple sessions using different wi-fi access points or a number of applications on a device opening separate connections. A session may also use mobile data for some periods where the

Mobile

Instead of the location/address of the broadband router the following data may additionally be captured:

- Cell mast name
- Cell mast sector
- Cell mast locations
- Network maps
- 2G/3G/4G coverage maps
- Device identifiers (e.g. MAC address, IMSI, IMEI) of the device connecting to the mobile internet – e.g. phone, tablet, dongle
- Device identifiers (e.g. MAC address) of any other devices using the internet through that connection (some devices can broadcast their signal allowing another device to use their connection).
- A handshake between a phone and a cell mast so the network knows where to route a mobile data session
- The url of a webpage in a browsing session (e.g. www.bbc.co.uk/news/story or news.bbc.co.uk or friend'sname.facebook.com)
- The content of the webpages being viewed, including any text, images, audio and videos embedded in the page
- The names and content of any files transmitted over a peer to peer connection
- Private posts being transmitted to or viewed on a webserver *
- A like message being posted on social media *

NB – in practice an internet access provider is often unable to distinguish what traffic it is carrying from a source IP to a destination IP.

• Device identifiers linked to a communication • Volumes of data uploaded/downloaded • Location/address of access point such a broadband router	data in the next column will be relevant	• NAT/PAT logs NB – what may appear to a customer to be a single mobile internet session may be multiple sessions for the same reasons as for public wi-fi access.	
Internet applications (such as Internet Telephony, Internet email)			
• Routing information • Name of a customer • Address of a customer • Phone number of a customer • Email address linked to a customer's account • Time/date/location at logon/logoff/reconnect	• Account details used to pay for the service • User name (or other credentials used to access the service)*** • Password • Billing data	• Email address of the sender or recipient of an email • Caller and callee for voip calls • Source IP address and port number • Message type (e.g. email, IM) • Time/date/location of each internet communication	• The body of an email • The subject line of an email • Any attachments to an email • The audio/ visual of an internet call • The messages comprising a conversation in an internet chat

.

* This only deals with looking at a communication which is viewing or uploading such posts. The posts themselves hosted on the servers of such a service would be out of scope of this section.

** This may be third party data when seen by an internet access provider

*** Certain online services can use identifiers of the device to verify a connection rather than a user inputting a username and password each time they use the service.

ANNEX B: Request Filter and ICRs

REQUEST FILTER OVERVIEW

INTRODUCTION

1. The request filter is an **additional communications data safeguard** being introduced in the Investigatory Powers Bill. It will work alongside other acquisition safeguards and existing infrastructure to prevent communications data from being provided to a public authority that is not directly relevant to a communications data request.

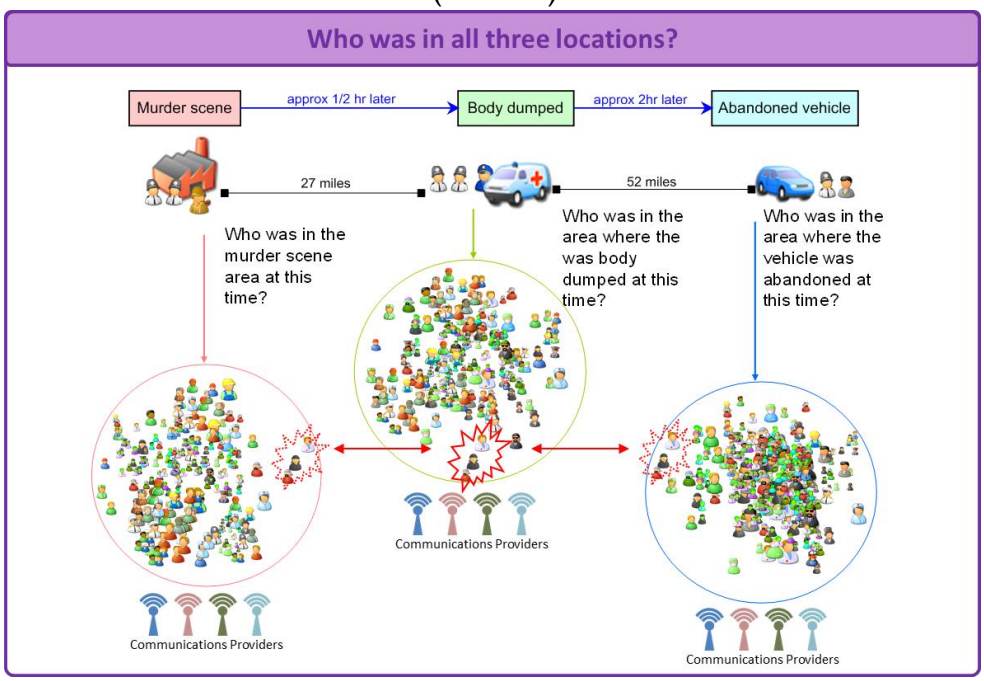
2. The request filter will **only process specified communications data** defined in a targeted communications data authorisation. The specified data must be necessary and proportionate for the operational requirement set out in the authorisation. The request filter is not a data mining tool or a search engine as it can only operate on limited sets of authorised data using specified and authorised processing steps. The request filter will not retain any communications data acquired for an authorisation once the processing for that authorisation is complete or it is no longer necessary to retain the data for the purpose of the authorisation.

3. The request filter is **available to all public authorities** to assist in accessing the communications data that they are permitted to use, subject to individual authorisations. With the increasing use of a wider range of online communications services and communications networks, the communications data required to answer investigative questions is becoming more fragmented. The filter arrangements will support complex communications data investigations. When a public authority makes such a request, they will only see the data they need to. Any extraneous data will be deleted and not made available to the public authority, thus limiting the collateral intrusion.

SCENARIO – MULTI-SCENE MURDER INVESTIGATION

4. An example where the filter arrangements might be used is for a serious crime involving multiple locations. This scenario involves three locations associated with a murder; the murder scene where the attack took place, the location where the body was discovered, and the location of an abandoned vehicle that has been connected with the murder.

5. The use of communications data is considered appropriate to establish who was in all three locations at the times of interest.



6. In this case the distances between the locations, and the limited time periods of interest at each location, mean that it is unlikely that individuals not involved in the murder would be at each of the locations at the specified times.

OPERATION OF THE REQUEST FILTER

7. The operation of the request filter involves a number of key steps which ensure that the public authority has the information necessary to make informed decisions about its request while the request filter provides the necessary safeguards. This is illustrated in the figure overleaf.

Step 1: Authorisation

8. The Applicant or SPoC may identify that the request filter will be used in a communications data request in order to safeguard privacy by limiting or managing collateral intrusion. The Designated Senior Officer will consider the necessity and proportionality of the application including the proposed use of the request filter. An application would identify both the data that will be disclosed to the request filter and the processing steps that will be used. The request filter may provide the Designated Senior Officer with additional information to inform consideration of the proportionality of the request.

9. As with other requests, the Designated Senior Officer may place constraints on the release of any results from the filter so that if the number of results is greater than authorised, disclosure to the Public Authority will be prevented.

Step 2: Acquisition

10. The request is sent to the filter which in turn acquires the authorised communication data for the request from the relevant communications providers. The communications providers will not be aware of the detail of the processing to be undertaken (as now for data released to public authorities) and will only disclose the communications data to the request filter.

Step 3: Processing

11. The request filter performs the authorised processing of the communications data that has been disclosed to produce a results file. The only communications data that is processed is that disclosed by the communications providers for the purpose of the relevant authorisation. Only the results from the filter processing are released to the SPoC. An additional check may be used prior to release to confirm that the number of results are within authorised limits.

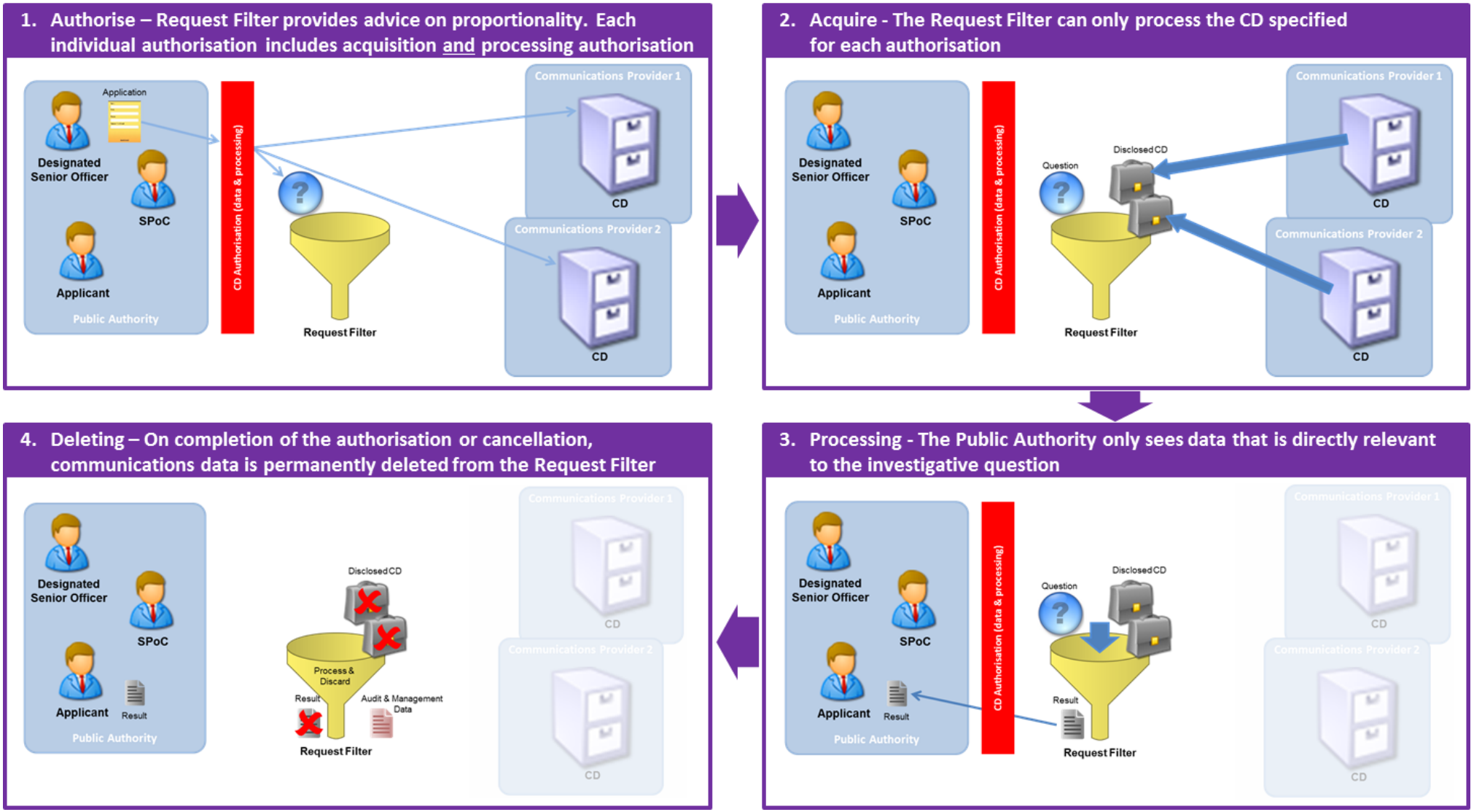
12. Because the data processed is limited to that which has been specified and authorised as necessary and proportionate for the operational requirement, the request filter will not operate as a data mining tool or search engine.

Step 4: Deletion

13. Once the results have been released and the authorisation is complete, the disclosed communications data (including the results) is deleted from the request filter. Only data required for audit and management information purposes as set out in the IP Bill is retained in the filter. The Secretary of State will produce an annual report on the operation of the request filter and will additionally report any significant errors immediately to the Investigatory Powers Commissioner.

REQUEST FILTER IMPLEMENTATION

14. The request filter will be established and maintained by the Secretary of State, effectively in the Home Office (although there is provision to transfer its functions to another public authority), sitting between a communications service provider and public authorities. Its operation and development will be overseen by the Investigatory Powers Commissioner.



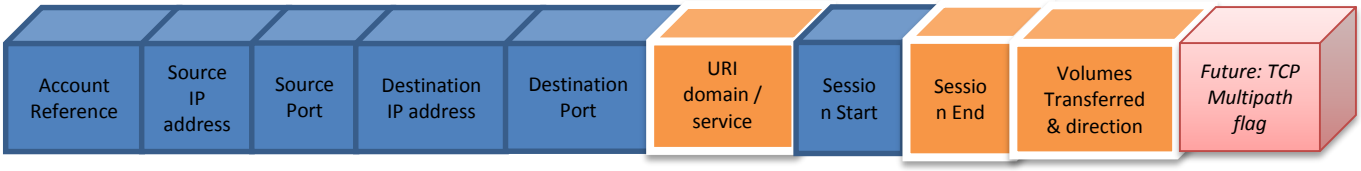
Request filter operation – summary of key steps

What is an Internet Connection Record?
This document addresses what an Internet Connection Record (ICR) is.

Internet Connection Records is a record of the internet services a specific device is connected to, such as a website or instant messaging application. It is captured by the company providing access to the internet.

Each ICR is a record of a single Internet Protocol event that occurs during the communication process and is made up of a number of components of communications data.

What is an Internet Connection Record composed of?
An Internet Connection Record can include the following components:



The components in blue form the core of an ICR.

The components in green are information entities whose quality may be degraded by a number of factors. These are desirable and will be sought where feasible and cost effective to do so.

Account reference, source IP address and port, session start, session end and volumes can already be retained under existing legislation.

The URI domain or service identifier may, depending on how a CSP configures its network, constitute 3rd party data. Unless a CSP process that data themselves for business purposes it cannot be retained as part of an ICR.

The component in pink is a foreseeable addition that may need to be incorporated in future.

A simple example ICR is shown for a mobile phone (the client).

Data Fields	Example	What does it represent?
Account Reference	13109976224	The mobile telephone number
Source IP : Port – Private	10.13.26.70 : 5256	What the client looks like to the Communication Service Provider for Internet access.
Source IP : Port - Public	232.99.52.12 : 80	What the client looks like to the Internet.

Destination IP : Port	135.20.32.87 : 80	The Internet Service being accessed by the client.
URI domain	www.socialmedia.com	The Internet Service's web domain.*
Service identifier	Social Media	The Internet Service's name.
Session Start Time	14:30:01 GMT 03/09/2015	The time and date for the start of session.
Session End Time	14:40:29 GMT 03/09/2015	The time and date for the end of session.
Data Volumes Transferred	1253 outgoing	The number of Bytes Transferred and direction.

* A URI retained as part of an ICR may only contain the elements of the address which identify the communication service concerned.

ANNEX C: Investigatory Powers Bill: Technical Advisory Board (TAB)

Legislative Basis

1. Clause 183 of the draft Investigatory Powers Bill replicates section 13 of the Regulation of Investigatory Powers Act 2000 (RIPA) which established the Technical Advisory Board (TAB), an advisory Non-Departmental Public Body. The TAB provides an important safeguard for communications companies and the Government, and ensures that any disputes that arise from certain obligations imposed on communications companies can be resolved satisfactorily.

2. Under RIPA, the TAB could be asked to consider the reasonableness of section 12 notices which place obligations on communications service providers to maintain permanent interception capabilities. Under the draft Bill, the TAB's remit will be extended. A right of appeal will apply to a technical capability notice, a national security notice, and a data retention notice. A technical capability notice places obligations on CSPs to provide permanent technical capabilities in relation to any of the following: interception, equipment interference, or communications data acquisition.

3. The following outlines the proposed functions and membership requirements of the TAB as established under the draft Bill.

Purpose

4. Under the draft Bill, the TAB will have two key functions:

i. Section 189 of the draft Bill allows the Secretary of State to makes regulations imposing obligations on communications service providers to maintain the technical capability to give effect to warrants or communications data authorisations. Before making such regulations the Secretary of State must consult with the TAB.

ii. CSPs will be able to seek a review of obligations placed upon them (in technical capability notices, national security notices, and data retention notices) by the Secretary of State. The Secretary of State may by regulation set out the circumstances in which a review may be sought. In such cases, the Secretary of State must consult the TAB and the Investigatory Powers Commissioner (IPC). The TAB must consider the technical requirements and financial consequences for the operator who made the referral. The TAB must give the operator concerned the opportunity to provide evidence and must report their conclusions to the both the operator and the Secretary of State. After considering reports from each, the Secretary of State may either vary or withdraw the notice, or confirm its effect.

Membership

5. The membership of the TAB is provided for in the Regulation of Investigatory Powers (Technical Advisory Board) Order 2001. This will be replaced by new regulations under the draft Bill which will be published in draft at the time of the introduction of the draft Bill. TAB membership requirements are being reviewed following the proposed extension of the TAB's remit to ensure that Board members have sufficient knowledge to advise the Secretary of State on the cost implications and technical feasibility of implementing a notice in the event of an appeal.

6. The TAB currently comprises 13 people: six representatives of communications service providers, six representatives of the intercepting agencies and an independent Chair. It is the Government's intention to maintain the size and balance of the TAB.

7. The TAB industry members must hold an office, rank or position within a communications service provider (or within a body representing such a provider's interests, such as a trade body) that is likely to be subject to obligations under:

- Clause 71 to retain relevant communications data
- Clause 189 to maintain permanent technical capabilities; or
- Clause 190 to comply with a national security notice,

8. Agency members must hold office, rank or position within one of the intercepting agencies (or in a body representing their interests, e.g. NTAC). The anonymity of agency members will be maintained.

9. There will be no obligation to have a representative from each intercepting agency or each CSP subject to obligations on the Board, in the line with the existing position.

10. The draft Bill and TAB Terms of Reference make clear that the TAB Chair cannot be a current employee of a communication service provider, an intercepting agency, or an organisation representing the interests of either category of people.

11. It is a requirement in the TAB's Terms of Reference that Board members are security cleared to a standard deemed appropriate by the Secretary of State. In addition, members must comply with the TAB's Code of Conduct[413].

12. Recruitment of the TAB Chair and industry members will be conducted in accordance with guidance provided by the Office for the Commissioner for Public Appointments. communications service providers on whom a notice (technical capability, national security or data retention notice) is likely to be imposed will be eligible to nominate candidates to fill vacant TAB posts. For appointments representing the intercepting agencies, candidates will be nominated by the intercepting agencies and appointed by the Home Secretary.

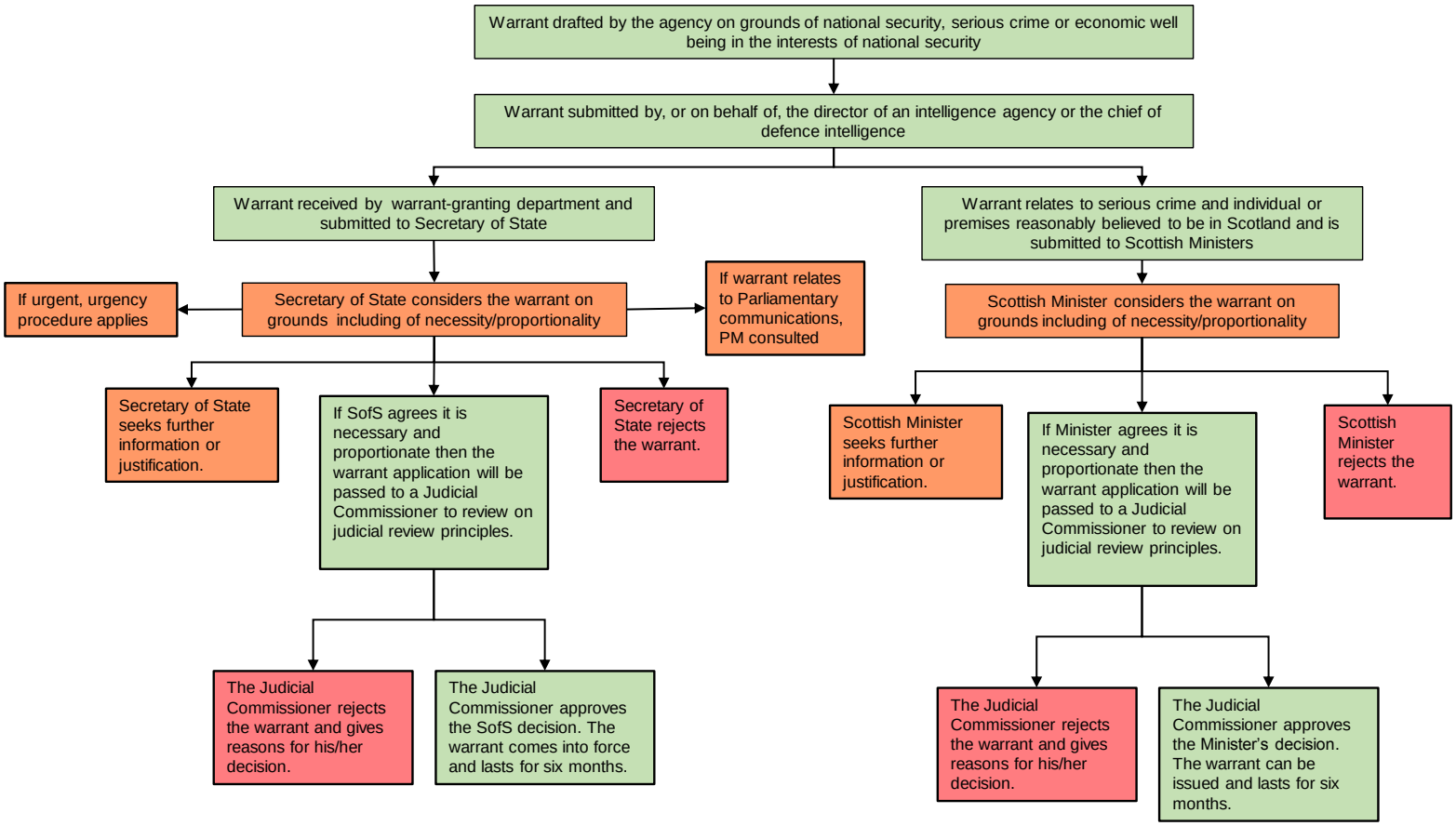
13. The working practices of the TAB will be set out clearly in the Terms of Reference. These will be remade and available in draft at the time of the introduction of the draft Bill. The working practices will include detail on the minimum representation required for the TAB to perform its duties and the timeframe in which it would consider any appeal.

[413] Current versions of the TAB Terms of Reference and Code of Conduct are publicly available on the TAB's website: https://www.gov.uk/government/organisations/technical-advisory-board

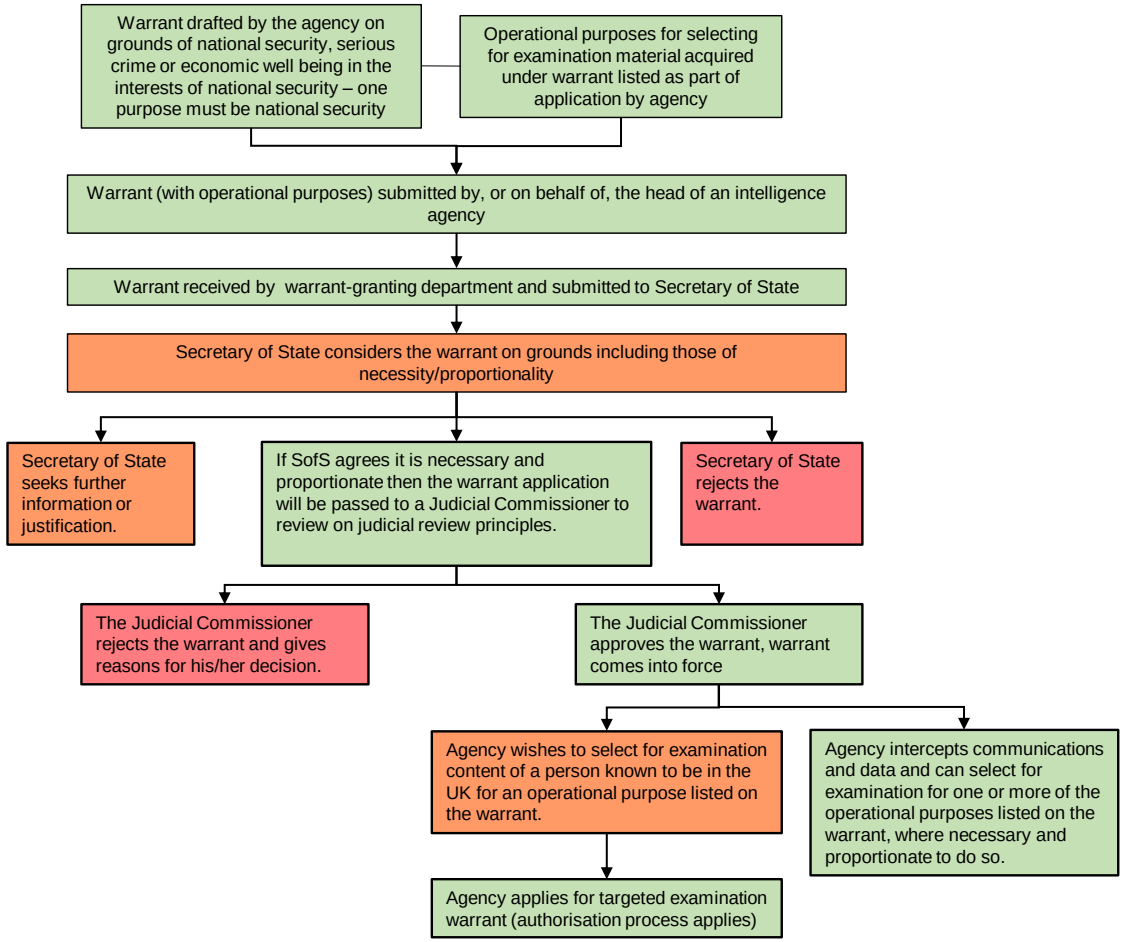
Annex D Authorisation processes for the Investigatory Powers Bill

Interception

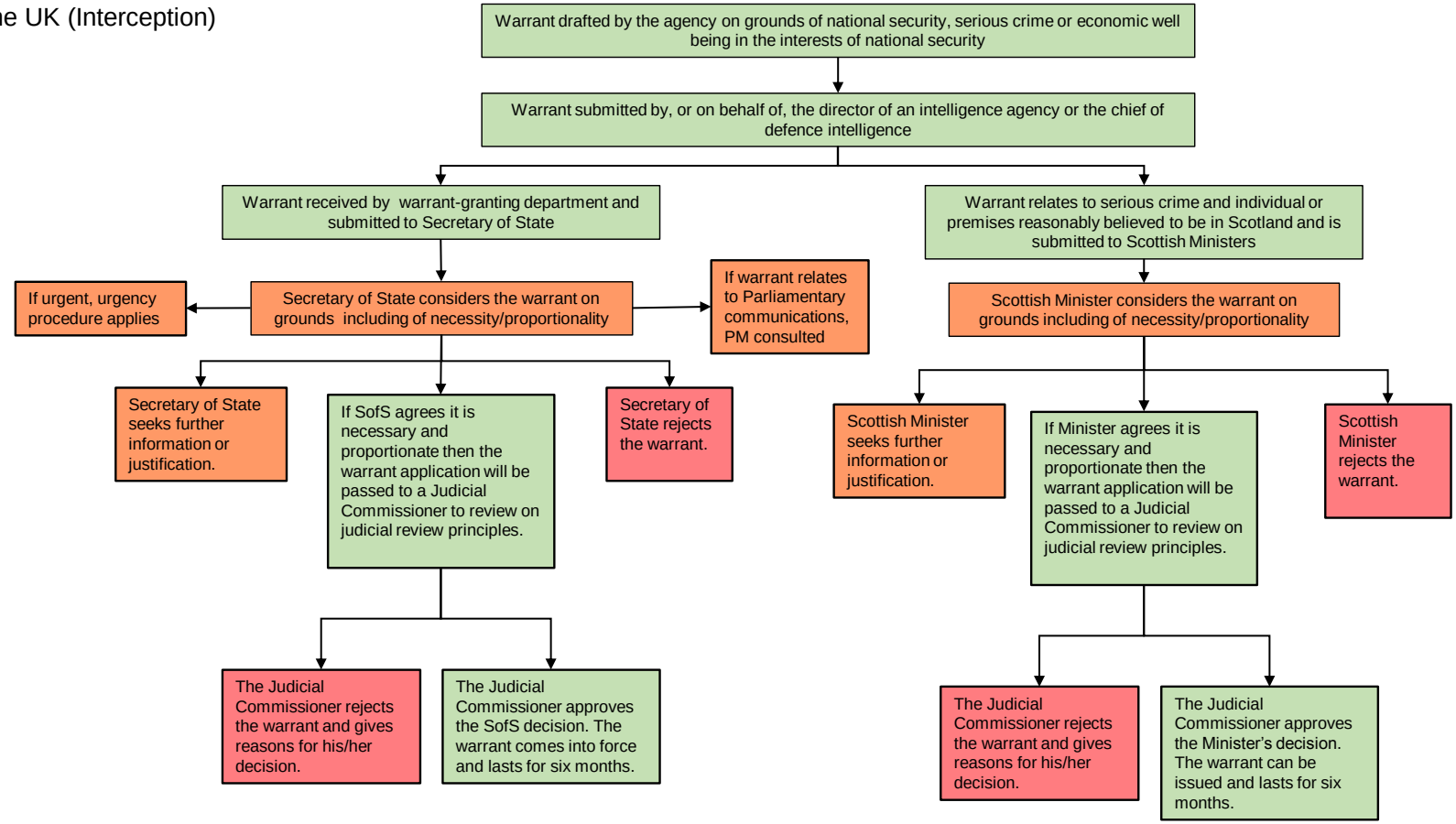
Targeted interception warrant



Bulk interception and related communications data (security and intelligence agencies)

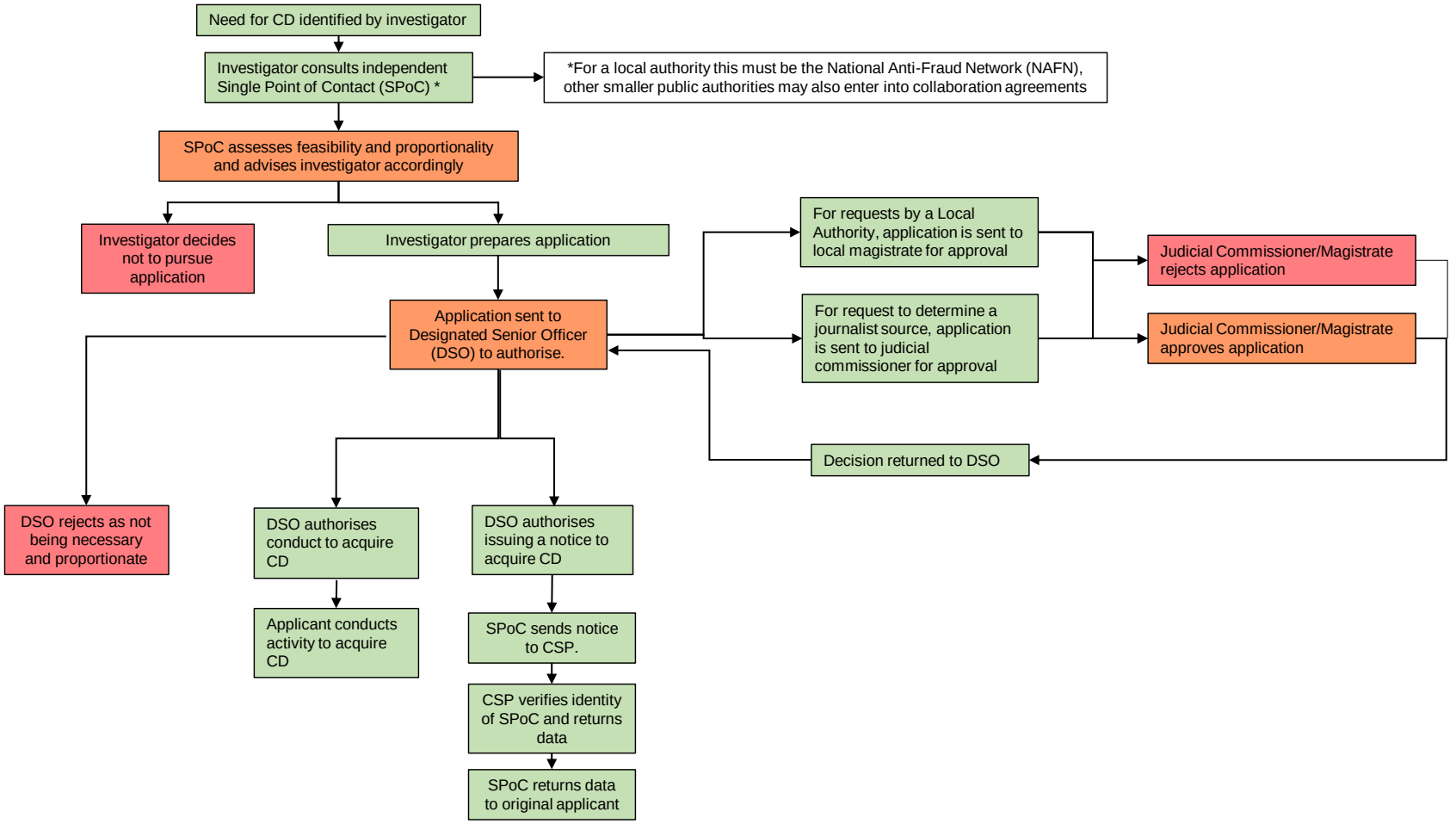


Targeted examination warrant authorising the selection for examination of content of persons in the UK (Interception)

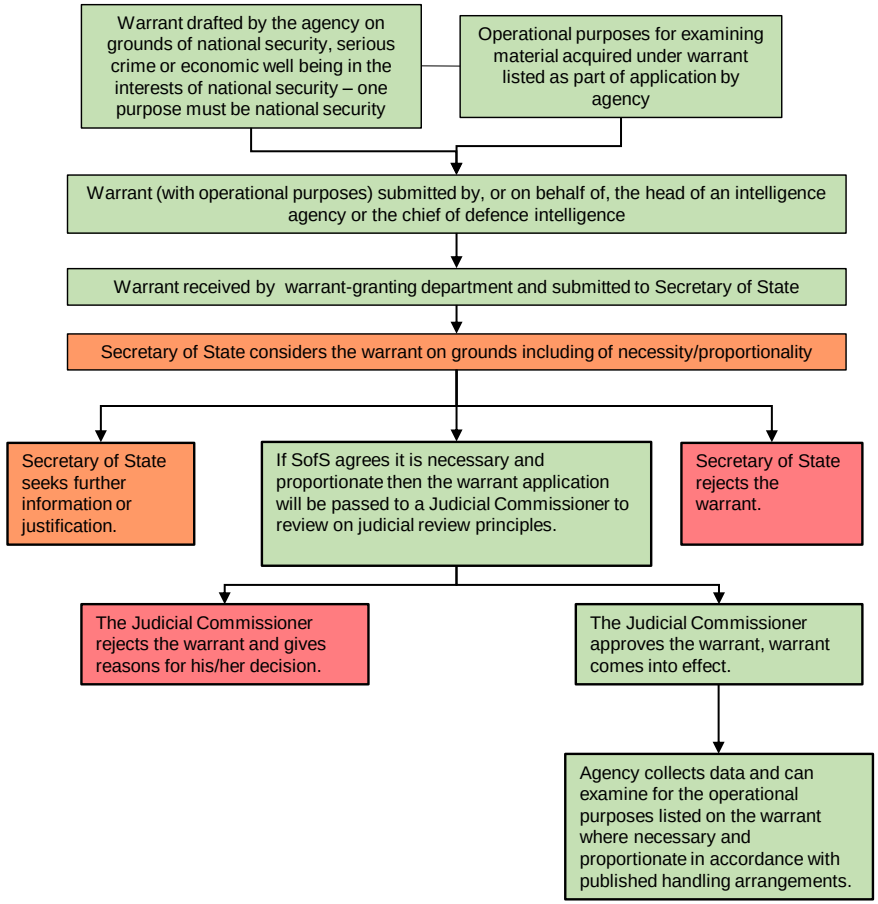


Communications data

Acquisition of targeted CD (public authorities)

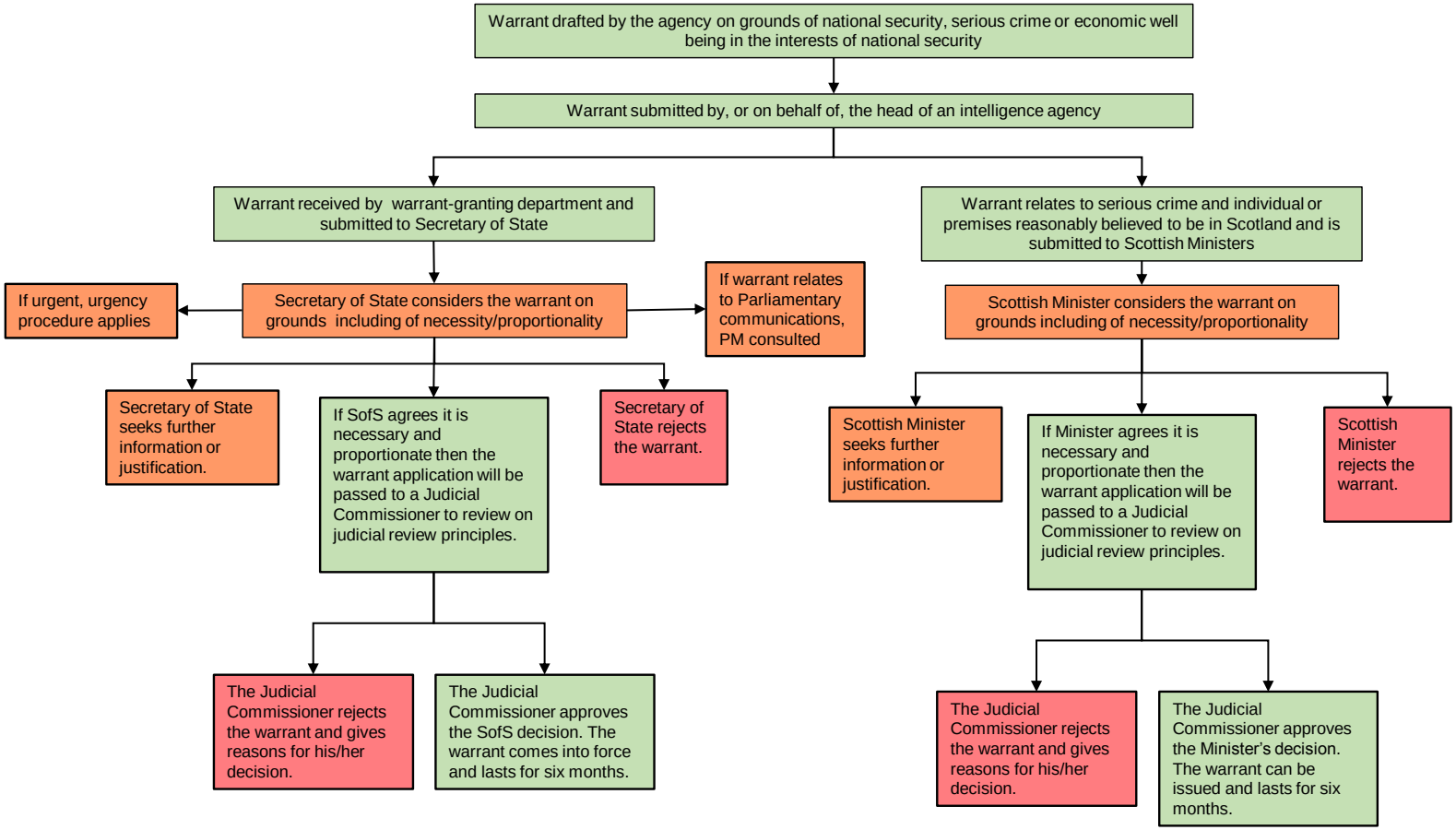


Bulk communications data (security and intelligence agencies)

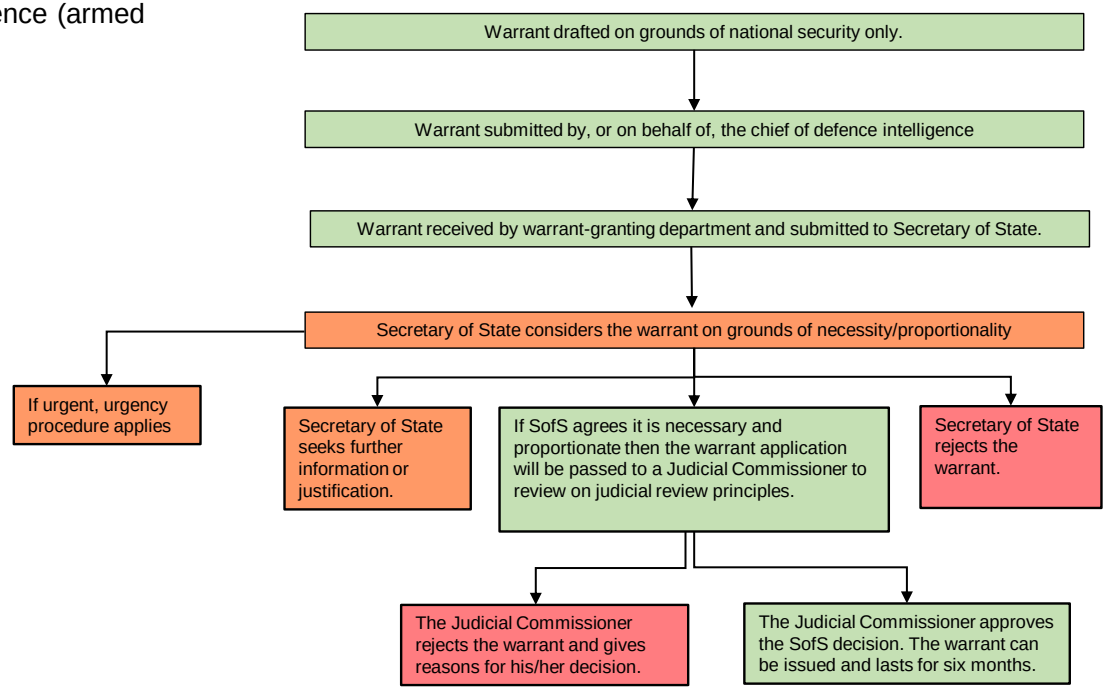


Equipment interface

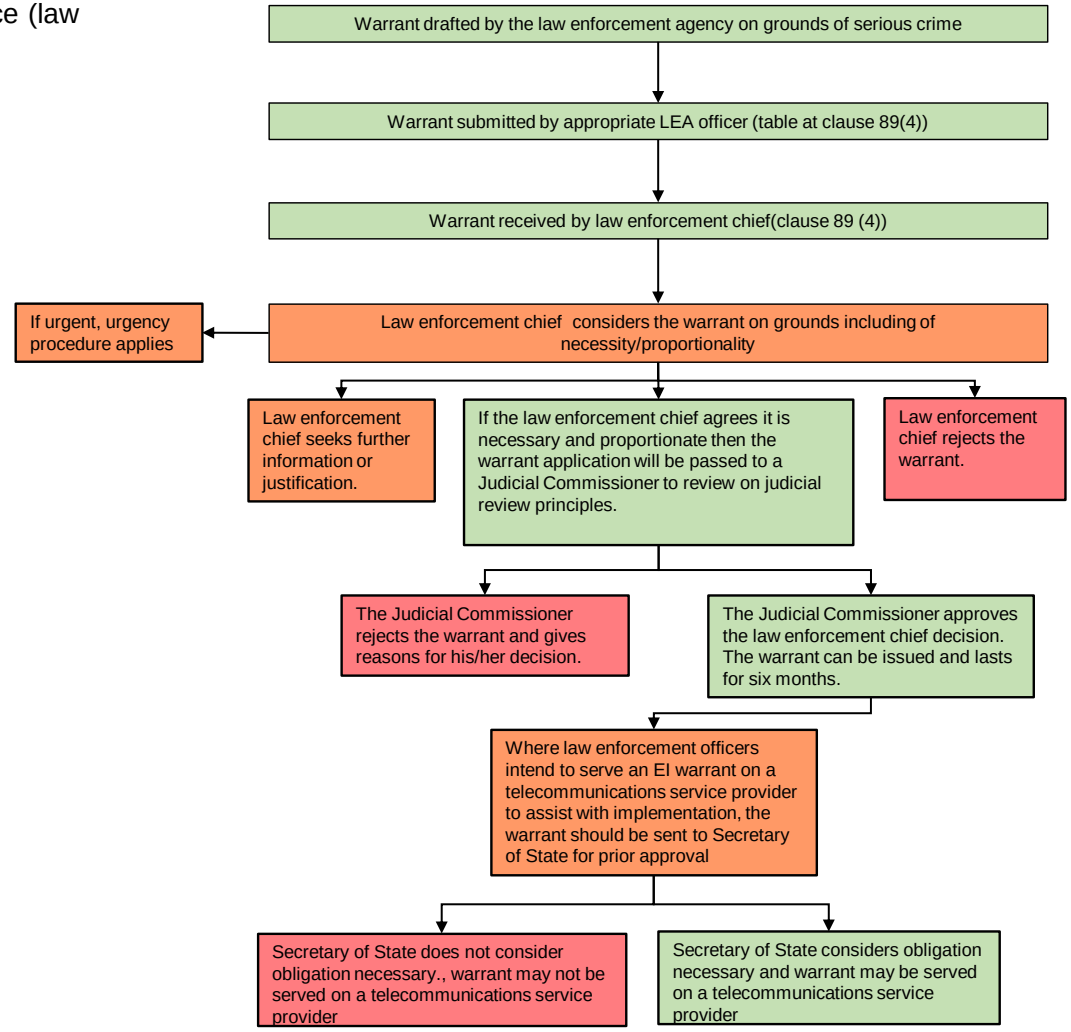
Targeted equipment interference warrant (security and intelligence agencies)



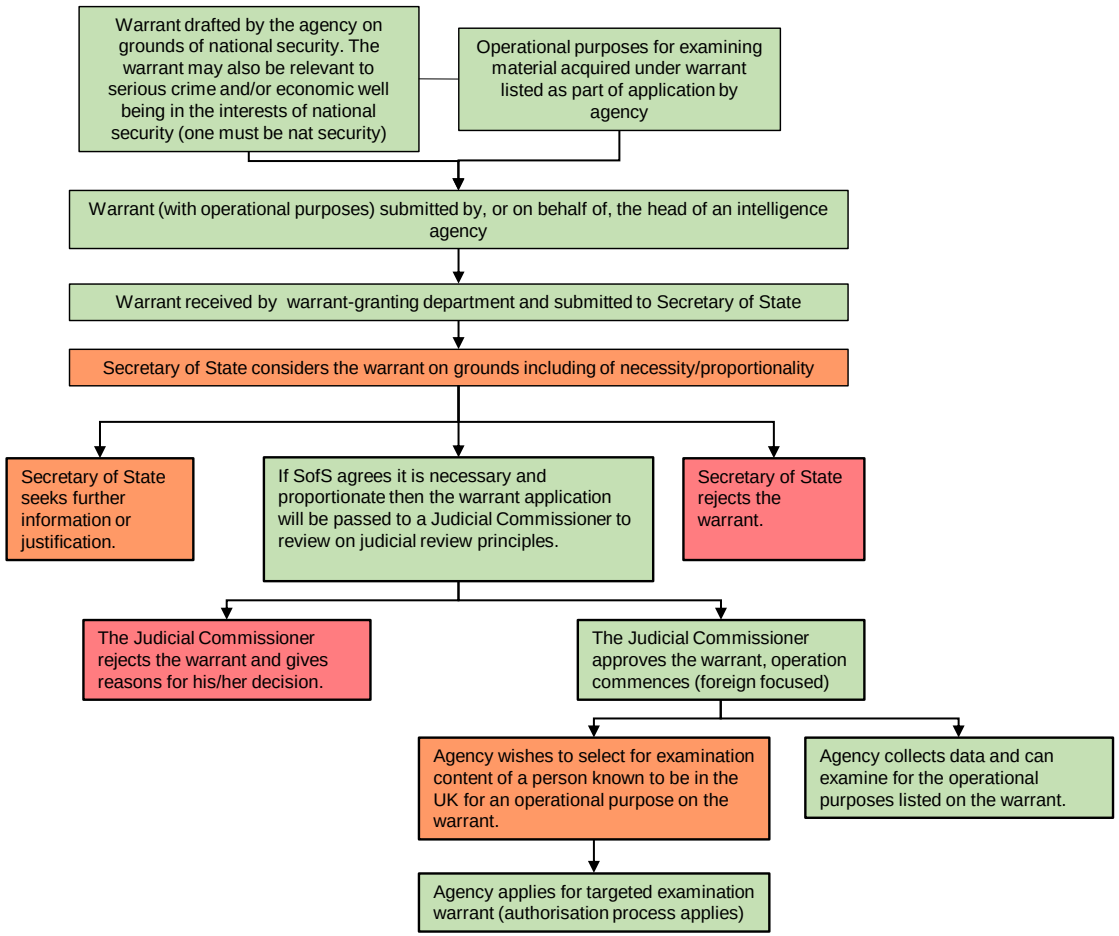
Equipment Interference (armed forces)



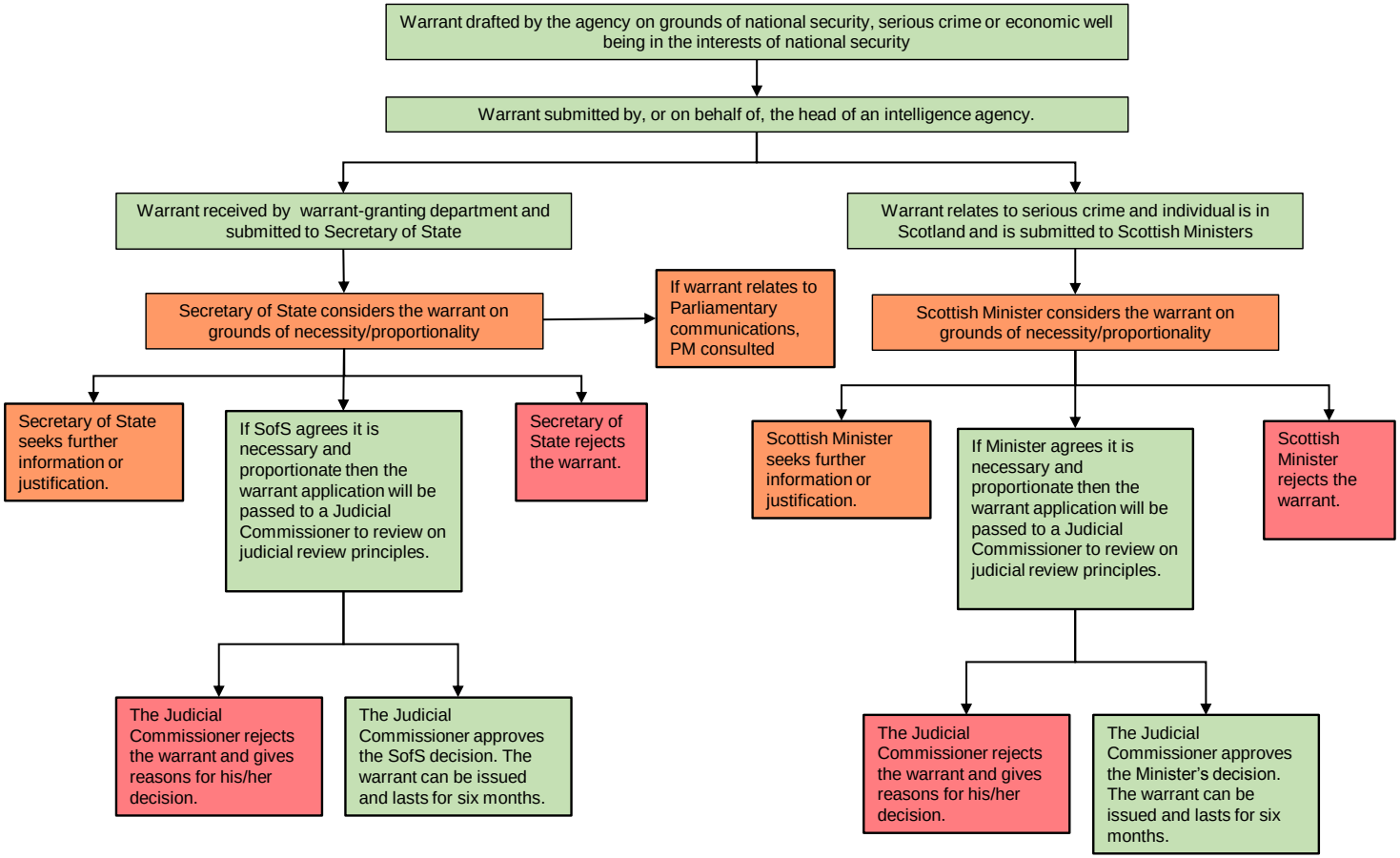
Equipment Interference (law enforcement)



Bulk Equipment Interference
(security and intelligence agencies)

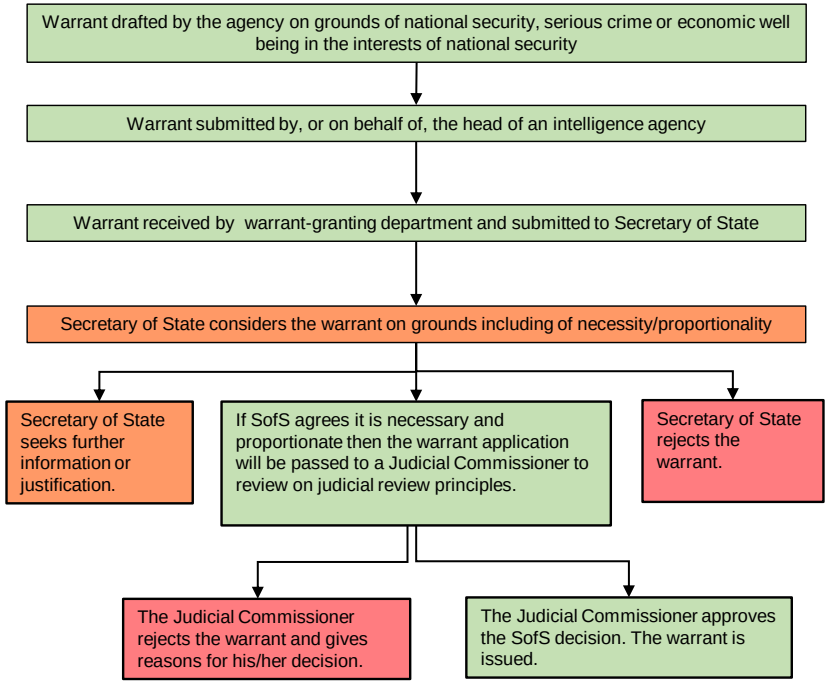


Targeted examination warrant (EI) authorising the selection for examination of content of persons in the UK



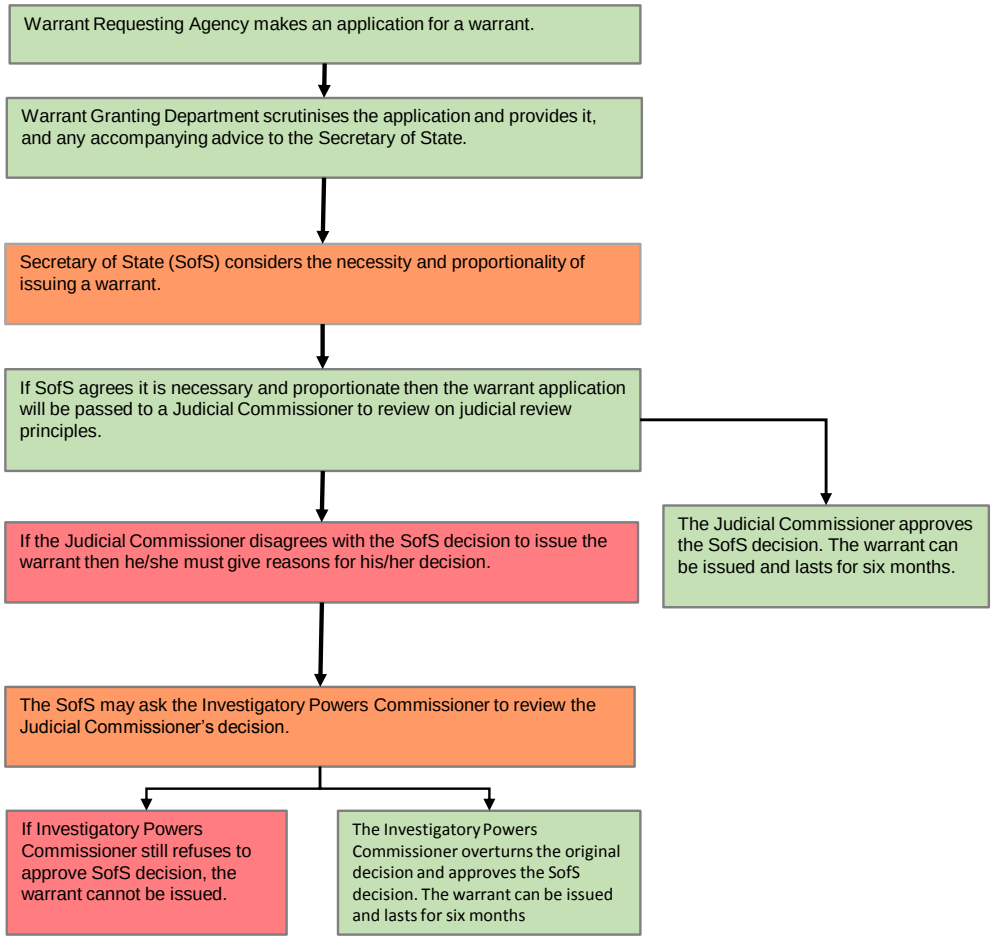
Bukk personal datasets

Bulk personal datasets (security and intelligence agencies)

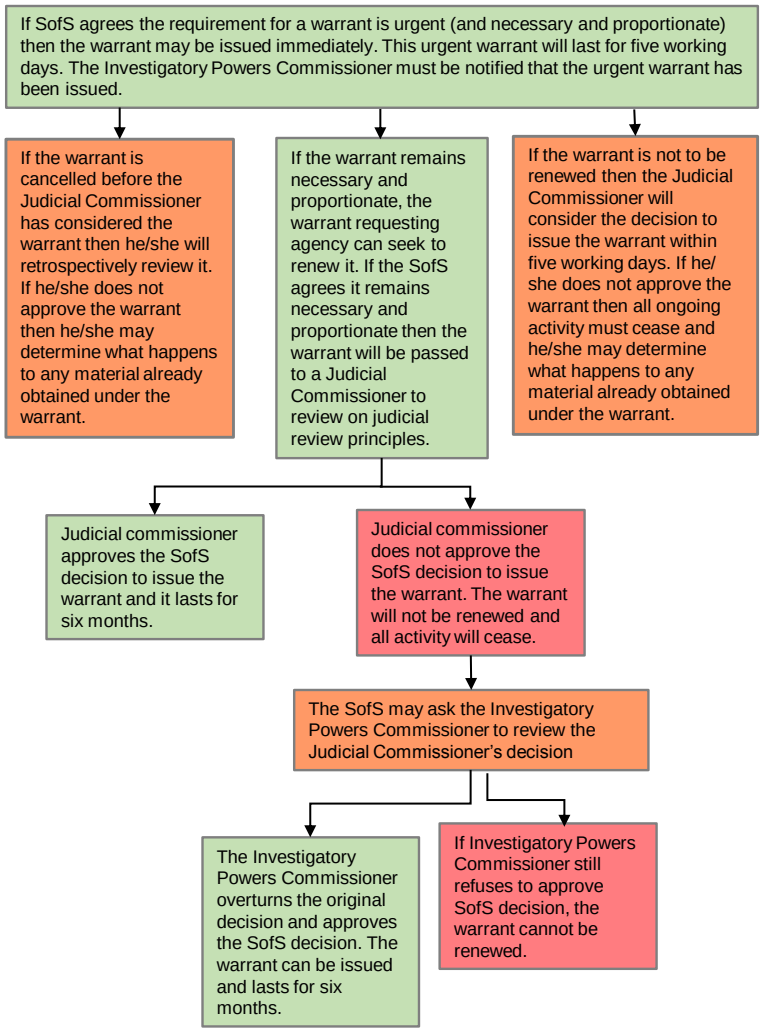


Urgency Procedures

Non urgent warrant



Urgent warrant



ANNEX E: Warrant Modifications

A major modification is one in which a name, premises, description, or organisation is either added or removed from a warrant. For example adding the extremist associate of a subject of intelligence interest to a warrant. A variation to a bulk warrant or an Equipment Interference warrant will always be considered a major modification.

A minor modification is the variation of a warrant that falls short of what is outlined above. For example if a subject of intelligence interest buys a new mobile phone, adding that second number to a warrant.

A major modification may be made by a Secretary of State, a member of the Scottish Government, a senior official acting on behalf of the Secretary of State or member of the Scottish Government. Where a major modification is made by a senior official then the relevant Secretary of State or member of the Scottish Government must be informed about the modification.

A minor modification may be made by anyone who can make a major modification as well as the person to whom the warrant was addressed or a senior person within the same public authority who was granted the warrant. Allowing a warrant requesting agency to make minor modifications ensures that the system is operationally efficient.

It will be for the warrant requesting agency to initially consider whether the modification being sought is minor or major. Guidance on this will be contained the Code of Practice.

All warrants, whether they have been modified or not, will still be subject to retrospective oversight by the Investigatory Powers Commissioner. We anticipate that the Commissioner will report annually on this aspect of their work, and would make it clear if they felt that the modification process was not being used appropriately. The current senior judicial figures who provide statutory oversight to the warrantry process have been consistently complementary about the rigour of the current regime and there has never been a suggestion that the urgency procedure has been abused.

Summary table of authorisation levels of warrantry

Type of warrant	*Legal instruments (we envisage this being explained in the relevant Codes of Practice)*	*Explanation*	*Authorisation level*	*Who can modify? (this does not include the power to remove, delete or cancel)*
Targeted Interception	Instrument	This will authorise both the acquisition of, and access to, the content of communications content and any related communications data. It will set out the statutory purposes and the legal test that the SofS must be personally satisfied has been met.	Secretary of State issues with Judicial Commissioner approval.	Not possible to modify the instrument.
	Schedule of subjects	Schedule sets out the name or description of a person, organisation or set of premises that is to be intercepted.	Authorised alongside the application and instrument when the warrant was authorised.	A change to this schedule would be a major modification. As such, it could be made by a senior official in the Warrant Granting Department. Subject to retrospective Judicial Commissioner oversight.
	Schedule of identifiers	This schedule sets out the communications selectors associated with the subject(s) of the warrant to be intercepted or a description of the factors that identify what needs to be	Senior official in either the Warrant Granting Department or Warrant Requesting Agency.	A change to this schedule would be a minor modification. As such, it could be made by a senior official in the Warrant Granting Department or the Warrant Requesting Agency.

		intercepted. There would be a schedule per CSP which will be served on the relevant CSP. The selectors could include factors that enable the communication address to be identified.		Subject to retrospective Judicial Commissioner oversight.
Targeted Examination Warrant	Instrument	This will authorise the examination of intercepted material obtained under a bulk interception warrant for persons believed to be in the UK.	Secretary of State issues with Judicial Commissioner approval.	Not possible to modify the instrument.
	Schedule of subjects	Schedule setting out the name or description of a person, organisation or set of premises.		A change to this schedule would be a major modification. As such, it could be made by a senior official in the Warrant Granting Department. Subject to retrospective Judicial Commissioner oversight.
Targeted Equipment Interference	Instrument	This will authorise both the acquisition of, and access to, the electronic communications, private data and equipment data. It will set out the statutory purposes and the legal test that the SofS must be personally satisfied has been met.	For Security and Intelligence Agency warrants, Secretary of State issues with Judicial Commissioner approval For Law enforcement warrants, Chief constable (or equivalent) with Judicial Commissioner approval.	Not possible to modify the instrument.

Schedule of subjects	Schedule setting out the subject matter of the warrants – e.g. equipment belonging to, used by or in the possession of a particular person, organisation or a group that shares a common purpose etc. The full list is provided in clause 83.	This would be authorised alongside the application and instrument when the warrant was authorised.	A change to this schedule would be a major modification (the Bill does not distinguish between minor and major modifications for EI, but it is equivalent to a major interception modification). For Security and Intelligence Agency (SIA) , modifications can be done by a senior official in the Warrant Granting Department. For Law Enforcement Agency (LEA) warrants, a Judicial Commissioner would authorise modifications. Both SIA and LEA warrants are subject to retrospective Judicial Commissioner oversight.
Schedule of actions and equipment	Schedule setting out specific actions that are authorised (i.e. IT attack / IMSI grab etc) and the associated equipment (e.g. phone).	This would be authorized alongside the application and instrument when the warrant was authorised.	A change to this schedule would be treated as a major modification (the Bill does not distinguish between minor and major modifications for EI, but it is equivalent to a major interception modification). For SIA warrants, modifications can be done by a senior official in the Warrant Granting Department. For law enforcement warrants, a Judicial

				Commissioner would authorise modifications. Both SIA and LEA warrants are subject to retrospective Judicial Commissioner oversight.
Equipment Interference Examination Warrant	Instrument	This will authorise the examination of material collected under a bulk EI warrant of persons believed to be in the UK.	Secretary of State issues with Judicial Commissioner approval.	Not possible to modify the instrument.
	Schedule of subjects	Schedule setting out the subject matter of the examination warrant – e.g. equipment belonging to, used by or in the possession of a particular person, organisation or a group that shares a common purpose etc.	This would be alongside the application and instrument when the warrant was authorised.	The Bill does not, currently, provide for modifications.
Bulk Equipment Interference / Interception / communications data	Instrument	This will authorise the collection of data in bulk and the circumstances in which the data can be selected for examination.. It will set out the statutory purposes for which data can be collected. . Only available to the Security and Intelligence Agencies.	Secretary of State issues with Judicial Commissioner approval.	Not possible to modify the instrument.
	Schedule of Bulk access conditions	This schedule will set out the operational purposes for which	This will be authorized alongside the application	Adding or varying an operational purpose must be made by a Secretary of State which must be

		the data collected in bulk can be examined.	and instrument when the warrant was authorised.	approved by a Judicial Commissioner. Removing an operational purpose must be made by a Secretary of State or a senior official acting on behalf of a Secretary of State.
Class Bulk Personal Datasets (BPD)	Instrument	This will authorise the acquisition of, and access to, the bulk personal datasets. It will set out the statutory purposes, the description of the class of BPDs that are being sought (etc.); and the legal test that the SofS must be personally satisfied has been met.	Secretary of State issues with Judicial Commissioner approval.	Not possible to modify the instrument.
	Schedule of Bulk access conditions	This schedule would set out the operational purposes which the intelligence agency can access the bulk personal datasets for.	This would be alongside the application and instrument when the warrant was authorised.	Major modifications (adding or varying an operational purpose) must be made by a Secretary of State or a senior official acting on behalf of a Secretary of State, and must be approved by a Judicial Commissioner. Minor modifications (removing an operational purpose) must be made by a Secretary of State, a senior official acting on behalf of a Secretary of State, the head of an intelligence service, or a

				senior official in the intelligence service.
Specific BPD	Instrument	This will authorise the acquisition of, and access to, a specified bulk personal dataset. It will set out the statutory purposes, a description of the bulk personal dataset that is being sought (etc.); and the legal test that the SofS must be personally satisfied has been met.	Secretary of State issues with Judicial Commissioner approval.	Not possible to modify the instrument.
	Schedule of Bulk access conditions	This schedule would set out the operational purposes which the intelligence agency can access the bulk personal datasets for.	This would be alongside the application and instrument when the warrant was authorised.	Adding or varying any operational purpose would be a 'major' modification (it is worth noting that a major BPD modification is different to a major interception modification). Such modifications can be made by the Secretary of State or a senior official in the Warrant Granting Department, and must be approved by a Judicial Commissioner. Removing an operational purpose would be a minor modification, and must be made by a Secretary of State, a senior official acting on behalf of a Secretary of State, the head of

	an intelligence service, or a senior official in the intelligence service. Subject to retrospective Judicial Commissioner oversight.

Annex F1

The table below provides an overview of how the Government has responded to the recommendations and conclusions in the ISC's Privacy and Security Report that are relevant to the draft Investigatory Powers Bill.

Recommendation		**Government Response**
A	The targeted interception of communications (primarily in the UK) is an essential investigative capability which the Agencies require in order to learn more about individuals who are plotting against the UK. In order to carry out targeted interception, the Agencies must apply to a Secretary of State for a warrant under Section 8(1) of RIPA. From the evidence the Committee has seen, the application process followed by MI5 is robust and rigorous. MI5 must provide detailed rationale and justification as to why it is necessary and proportionate to use this capability (including, crucially, an assessment of the potential collateral intrusion into the privacy of innocent people).	The Government welcomes the ISC's endorsement of the strong safeguards that apply to the targeted interception regime under existing legislation. These safeguards have been carried across to the provisions in Chapter 1 of Part 2 of the draft Investigatory Powers Bill and will be strengthened by the application of further safeguards.
B	GCHQ and SIS obtain fewer 8(1) warrants. When they do apply for such warrants, they do so via a submission to the Foreign Secretary. While this submission covers those aspects required by law, it does not contain all the detail covered by MI5's warrant applications. We therefore recommend that GCHQ and SIS use the same process as MI5 to ensure that the Home Secretary and the Foreign Secretary receive the same level of detail when considering an 8(1) warrant application.	The Government agrees that there should be consistency in processes and applications where appropriate. Part 2, Chapter 1 of the draft Bill provides a single, clear warrant granting regime and ensures consistency through the application of robust oversight and authorisation arrangements for all agencies that use interception powers. The draft Bill provides for targeted interception warrants and targeted examination warrants (clause 12).

		Further details will be in Codes of Practices, which will be published in draft on formal introduction of the Bill in 2016.
C	RIPA expressly prohibits any reference to a specific interception warrant. We do not consider this is proportionate: disclosure should be permissible where the Secretary of State considers that this could be done without damage to national security.	The Government recognises the importance of being as transparent as possible. The draft Bill provides for greater transparency than ever before by clarifying, within the constraints imposed by national security, the current restrictions and prohibitions relating to the disclosure of warrants and intercepted material (RIPA ss.15 and 19, Official Secrets Act 1989 s.4) in order to ensure, in particular, that: (a) there is no legal obstacle to explaining the uses (and utility) of warrants to Parliament, courts and public. Clause 43(5)(h) allows for the disclosure of information which does not relate to any specific warrant but relates to interception warrants in general. This will allow for the explaining of the uses and utility of warrants to Parliament, courts and the public. (b) as recommended by the Police Ombudsman for Northern Ireland in his report of 30 October 2014 on the Omagh bombing, there is "*absolute clarity as to how specific aspects of intelligence can be shared in order to assist in the investigation of crime*". Clause 40 imposes restrictions on the access to and disclosure of intercept material, limiting this to the minimum necessary for the authorised purposes. The authorised purposes include prevention

		or detection serious crime. This clause, in combination with s19 of the Counter-Terrorism Act 2008 (which includes provisions on the disclosure of information by the Intelligence Agencies) permits intelligence to be shared with law enforcement bodies in order to assist in the investigation of a serious crime.
D	The Agencies have described 'thematic warrants' as covering the targeted interception of the communications of a "defined group or network" (as opposed to one individual). The Committee recognises that such warrants may be necessary in some limited circumstances. However, we have concerns as to the extent that this capability is used and the associated safeguards. Thematic warrants must be used sparingly and should be authorised for a shorter timescale than a standard 8(1) warrant.	Clauses 13 and 83 of the draft Bill provide for 'thematic' warrants by enabling targeted interception and equipment interference warrants to be issued in relation to a specific operation or investigation. Such warrants will be subject to strict safeguards. Clause 23 of the draft Bill requires that operation-specific interception warrants should include details of the targets who are the subjects of those warrants. Clause 93 makes equivalent provisions in respect of equipment interference warrants. The overall warrantry authorisation regime is also being made more robust.
E	There are other targeted techniques the Agencies can use which also give them access to the content of a specific individual's communications. However, the use of these capabilities is not necessarily subject to the same rigour as an 8(1) warrant, despite providing them with the same result. All capabilities which provide the content of an individual's communications should be subject to the same legal safeguards, i.e. they must be authorised by a Secretary of State and the application to the Minister must specifically address the Human Rights Act 'triple test' of legality, necessity and proportionality.	The Government recognises the need to provide a single, clear warrant granting regime and to ensure consistency. Covert capabilities, such as the use of interception (including through Wireless Telegraphy) and equipment interference have been put on a clear statutory footing through Parts 2 and 5 of the draft Bill and will be subject to strict safeguards. Bulk interception and equipment interference powers are also available to the security and intelligence agencies and provided for in Part 6 of the draft Bill. Similar safeguards are set out in the Bill in relation to both targeted and bulk use of these powers. Ministers will be directed, through the Bill to only authorise a warrant where they are assured that it is both necessary and proportionate.

F	GCHQ's bulk interception capability is used either to investigate the communications of individuals already known to pose a threat, or to generate new intelligence leads, for example to find terrorist plots, cyber attacks or other threats to national security. It has been alleged – inaccurately – that this capability allows GCHQ to monitor all of the communications carried over the internet. GCHQ could theoretically access a small percentage (***%) of the 100,000 bearers which make up the internet, but in practice they access only a fraction of these (***%) – we detail below the volume of communications collected from these bearers. GCHQ do not therefore have 'blanket coverage' of all internet communications, as has been alleged – they have neither the legal authority, the technical capacity nor the resources to do so.	The Government welcomes the ISC's clarification that GCHQ does not have 'blanket coverage' of all internet communications, and that it only examines those communications that relate to its statutory purposes. This is provided for in Part 6 of the Bill at clauses 107 (bulk interception), 122 (bulk communications data acquisition), and 137 (bulk equipment interference) of the draft Bill. These statutory purposes are set out clearly in the draft Bill and limit examination to those situations where it is necessary in the interests of national security; for the purposes of preventing or detecting serious crime; or in the interests of the economic well-being of the UK so far as those interests are also relevant to the national security of the UK. Examination is only permitted for the statutory purpose the warrant has been issued. The draft Bill maintains the strong safeguards that apply to the bulk interception regime. It will strengthen existing statutory safeguards so that analysts will only be able to search for and examine communications where it is necessary in the pursuit of a specified operational purpose that has been authorised by the Secretary of State and approved by the Judicial Commissioner. This will apply irrespective of the person's nationality or location and will apply to both the content of communications and related communications data that may be intercepted under the bulk interception regime. Clause 119 provides that where an intelligence agency is investigating a person in the British Islands, the agency will need to obtain a targeted examination warrant under clause 12(1)(b)
G	It has been suggested that GCHQ's bulk interception is indiscriminate. However, one of the major processes by which GCHQ conduct bulk interception is targeted. GCHQ first choose the bearers to access (a small proportion of those they can theoretically access) and then use specific selectors, related to individual targets, in order to collect communications from those bearers. This interception process does not therefore collect communications indiscriminately.	
H	The second bulk interception process we have analysed involves the *** collection of large quantities of communications. ***. However, this collection is not indiscriminate. GCHQ target only a small proportion of those bearers they are able to access. The processing system then applies a set of selection rules and, as a result, automatically discards the majority of the traffic on the targeted bearers.	

I	There is a further filtering stage before analysts can select any communications to examine or read. This involves complex searches to draw out communications most likely to be of greatest intelligence value and which relate to GCHQ's statutory functions. These searches generate an index. Only items contained in this index can potentially be examined – all other items cannot be searched for, examined or read.	before it may examine the contents of that person's communications intercepted under a bulk warrant. Clause 147 applies similar safeguards in respect of data acquired under bulk equipment interference warrants.
J	Our scrutiny of GCHQ's bulk interception via different methods has shown that while they collect large numbers of items, these have all been targeted in some way. Nevertheless, it is unavoidable that some innocent communications may have been incidentally collected. The next stage of the process – to decide which of the items collected should be examined – is therefore critical. For one major method, a 'triage' process means that the vast majority (***%) of the items collected are never looked at by an analyst. For another major method, the analysts use the search results to decide which of the communications appear most relevant and examine only a tiny fraction (***%) of the items that are collected. In practice this means that fewer than *** of ***% of the items that transit the internet in one day are ever selected to be read by a GCHQ analyst. These communications – which only amount to around *** thousand items a day – are only the ones considered to be of the highest intelligence value. Only the communications of suspected criminals or national security targets are deliberately selected for examination.	The Government welcomes the ISC's conclusion that only the communications of suspected criminals or national security targets are deliberately selected for examination by GCHQ. Part 6 of the draft Bill maintains the strong safeguards that apply to the bulk interception regime and provides equivalent safeguards in respect of bulk communications data and bulk equipment interference. It strengthens existing statutory safeguards so that analysts will only be able to search for and examine communications where it is necessary in the pursuit of a specified operational purpose that has been authorised by the Secretary of State and approved by a Judicial Commissioner. This will apply to both the content of communications and related communications data that may be intercepted under the bulk regime.

K	It is essential that the Agencies can 'discover' unknown threats. This is not just about identifying individuals who are responsible for threats, it is about finding those threats in the first place. Targeted techniques only work on 'known' threats: bulk techniques (which themselves involve a degree of filtering and targeting) are essential if the Agencies are to discover those threats.	The Government welcomes the ISC's acknowledgement of the need to maintain the ability to find those who seek to cause harm to the United Kingdom and our citizens and interests abroad. Part 6 of the draft Bill provides a clear statutory basis for all of the 'bulk' powers used by the agencies for the purpose of discovering previously unknown threats, including the safeguards and oversight arrangements covering the use of these powers.
L	We are satisfied that current legislative arrangements and practice are designed to prevent innocent people's communications being read. Based on that understanding, we acknowledge that GCHQ's bulk interception is a valuable capability that should remain available to them.	The Government is grateful to the ISC for their conclusion that GCHQ's bulk interception capability is a valuable tool and that the current legislative arrangements and practices are designed to prevent innocent people's communications being read. Chapter 1 of Part 6 of the draft Bill carries across all of the existing safeguards that apply to the bulk interception regime. The draft Bill also reduces the number of agencies that can apply for a bulk interception warrant, enhances the authorisation regime and limits the purposes for which intercepted communications may be examined
M	While we recognise privacy concerns about bulk interception, we do not subscribe to the point of view that it is acceptable to let some terrorist attacks happen in order to uphold the individual right to privacy – nor do we believe that the vast majority of the British public would. In principle it is right that the intelligence Agencies have this capability, provided – and it is this that is essential – that it is tightly controlled and subject to proper safeguards.	The Government agrees that it is never acceptable to let terrorist attacks happen where they can be prevented. Chapter 1 of Part 6 of the draft Bill ensures the security and intelligence agencies maintain their vital bulk interception capabilities, which will be subject to enhanced safeguards, a more robust authorisation framework and strengthened oversight arrangements.

N	Bulk interception is conducted on external communications, which are defined in law as communications either sent or received outside the UK (i.e. with at least one 'end' of the communication overseas). The collection of external communications is authorised under 19 warrants under Section 8(4) of RIPA. These warrants – which cover the Communications Service Providers who operate the bearers – do not authorise the examination of those communications, only their collection. The warrants are therefore all accompanied by a Certificate which specifies which of the communications collected under the warrant may be examined. GCHQ are not permitted by law to examine the content of everything they collect, only that material which falls under one of the categories listed in the Certificate. In the interests of transparency we consider that the Certificate should be published.	The Government agrees that bulk interception is a vital tool designed to obtain foreign-focussed intelligence. There are strict safeguards governing the use of bulk interception, which ensure the agencies comply fully with their human rights obligations. Applications for bulk interception warrants will continue to be limited to the security and intelligence agencies and only for limited purposes. Proposals in the draft Bill mean that the Certificate will be replaced with a more detailed set of operational purposes for which material intercepted under a bulk warrant may be examined (clauses 107 and 119). Those operational purposes will be authorised in advance by the Secretary of State and approved by a Judicial Commissioner. In circumstances where the intelligence agencies wish to examine a communication of a person known to be in the British Islands they must apply to the Secretary of State for a targeted examination warrant. Publishing the categories of Operational Purposes in detail would be detrimental to national security.
O	8(4) warrants allow GCHQ to collect 'external communications' – these are defined in RIPA as communications where at least one end is overseas. However, in respect of internet communications, the current system of 'internal' and 'external' communications is confusing and lacks transparency. The Government must publish an explanation of which internet communications fall under which category, and ensure that this includes a clear and comprehensive list of communications.	The draft Bill implements the spirit of this recommendation in full; however the Government does not believe that the answer lies in trying to categorise all internet communications according to 'internal' or 'external' criteria. The draft Bill clarifies the current terminology, replacing the definition of 'external' communications with a new requirement that bulk interception warrants should only be authorised where there is a 'foreign focus' – i.e. where the intention is to acquire the communications of persons overseas (clause 106) .

P	The legal safeguards protecting the communications of people in the UK can be summarised as follows: • The collection and examination of communications with both ends known to be in the UK requires an 8(1) warrant. • All other communications can be collected under the authority of an 8(4) warrant. • Of these, GCHQ may search for and select communications to examine on the basis of a selector (e.g. email address) of an individual overseas – provided that their reason for doing so is one or more of the categories described in the 8(4) Certificate. • GCHQ may search for and select communications to examine on the basis of a selector (e.g. email address) of an individual in the UK if – and only if – they first obtain separate additional authorisation from a Secretary of State in the form of an 8(1) warrant or a Section 16(3) modification to the 8(4) warrant. • It would be unlawful for GCHQ to search for communications related to somebody known to be in the UK among those gathered under an 8(4) warrant without first obtaining this additional Ministerial authorisation. • This is reassuring: under an 8(4) warrant the Agencies can examine communications relating to a legitimate	The Government thanks the ISC for its helpful summary of the current safeguards that protect the communications of people in the UK. The draft Bill strengthens these further and requires that where an agency seeks to select for examination the communications of a person in the UK it will have to apply to the Secretary of State for a targeted examination warrant, which will need to be approved by a Judicial Commissioner before it can come into force (clause 119).

	overseas target, but they cannot search for the communications of a person known to be in the UK without obtaining specific additional Ministerial authorisation.	
Q	The nature of the 16(3) modification system is unnecessarily complex and does not provide the same rigour as that provided by an 8(1) warrant. We recommend that despite the additional resources this would require – searching for and examining the communications of a person known to be in the UK should always require a specific warrant, authorised by a Secretary of State.	The Government accepts this recommendation in full. The draft Bill strengthens the safeguards that apply to the communications of persons in the UK, requiring that where an agency seeks to select for examination the communications of a person in the UK it will have to apply to the Secretary of State for a targeted examination warrant, which will need to be approved by a Judicial Commissioner before it can come into force (clause 119).

R	While the protections outlined above apply to people in the UK, they do not apply to UK nationals abroad. While GCHQ operate a further additional system of authorisations, this is a policy process rather than a legal requirement. We consider that the communications of UK nationals should receive the same level of protection under the law, irrespective of where the person is located. The interception and examination of such communications should therefore be authorised through an individual warrant like an 8(1), signed by a Secretary of State. While we recognise this would be an additional burden for the Agencies, the numbers involved are relatively small and we believe it would provide a valuable safeguard for the privacy of UK citizens.	Whilst the Government understands the intention behind the ISC's recommendation it does not believe that there is an objective justification for different protections based purely on nationality. The draft Bill provides strong protections for the examination of content or communications data irrespective of nationality.
S	While the law sets out which communications may be collected, it is the selection of the bearers, the application of simple selectors and initial search criteria, and the complex searches which determine what communications are read. The Interception of Communications Commissioner should be given statutory responsibility to review the various selection criteria used in bulk interception to ensure that these follow directly from the Certificate and valid national security requirements.	The Government agrees that strong oversight of the use of investigatory powers is essential. That is why Part 8 of the draft Bill will reform oversight by creating a new Investigatory Powers Commissioner who will have the power to inspect any aspect of the security and intelligence agencies' use of investigatory powers that he or she considers appropriate, including selection criteria. In addition, a Judicial Commissioner will have a role alongside the Secretary of State in approving the operational purposes for which material collected in bulk can be examined.

T	From the evidence we have seen, there are safeguards in place to ensure that analysts examine material covered by the 8(4) Certificate only where it is lawful, necessary and proportionate to do so. GCHQ's search engines are constructed such that there is a clear audit trail, which may be reviewed both internally and by the Interception of Communications Commissioner. Nevertheless, we were concerned to learn that, while misuse of GCHQ's interception capabilities is unlawful, it is not a specific criminal offence. We strongly recommend that the law should be amended to make abuse of intrusive capabilities (such as interception) a criminal offence.	Unlawful interception is already a criminal offence under the Regulation of Investigatory Powers Act 2000 and clause 2 of the draft Bill replicates this provision. The deliberate misuse of any agency interception capability may also engage existing offences, including misfeasance in public office or offences under the Computer Misuse Act.
U	In our 2013 Report on the draft Communications Data Bill, we concluded that "it is essential that the Agencies maintain the ability to access Communications Data". The Committee remains of that view: it is a critical capability.	The Government shares the Committee's view that it is essential for the Agencies to maintain the ability to access communications data. Part 3 of the draft Bill provides a clear statutory basis for the acquisition of communications data and Part 4 provides for the retention of communications data, both subject to robust safeguards. Chapter 2 of Part 6 makes explicit provision for bulk acquisition of communications data and sets out safeguards that apply to related communications data acquired under the bulk interception regime.
V	The Committee considers that the statutory definition of Communications Data – the 'who, when and where' of a communication – is narrowly drawn and therefore, while the volume of Communications Data available has made it possible to build a richer picture of an individual, this remains considerably less intrusive than content. We therefore do not consider that this narrow category of Communications Data requires the same degree of protection as the full content of a communication.	The Government accepts that there is a need to clarify the different types of communications data and accepts the spirit of the ISC's recommendations. Clause 193 of the draft Bill includes revised definitions of the categories of communications data: - Entity data will include data about persons or devices, such as subscriber or billing information.

W	However, there are legitimate concerns that certain categories of Communications Data – what we have called 'Communications Data Plus' – have the potential to reveal details about a person's private life (i.e. their habits, preferences and lifestyle) that are more intrusive. This category of information requires greater safeguards than the basic 'who, when and where' of a communication.	- Event data will include data about interaction between persons or devices, such as the fact of a call between two individuals. Recognising the more intrusive nature of events data, Schedule 4 of the draft Bill requires authorisation of access to such data be at a more senior level than for entity data. In describing the communications data obtained, clause 71 of the draft Bill provides for the retention of internet connection records. The Government recognises the sensitive nature of internet connection records and for that reason clause 47 restricts the purposes for which they can be acquired further than other forms of communications data. A designated senior officer in a public authority will only be able to require disclosure or processing of internet connections records for the following purposes: - To identify the sender of an online communication. This will often be in the form of an IP address resolution and the internet service used must be known in advance of the application - To identify which communication services a person has been using. For example whether they are communicating through apps on their phone

		- To identify where a person has accessed illegal content. For example an internet service hosting child abuse imagery. Clause 71 of the draft Bill also provides that local authorities will not be permitted to acquire internet connection records under any circumstances. Before making a request for communications data, public authorities will need to consider which data type they require access to and whether it is necessary and proportionate to do so.
X	The Agencies' use Bulk Personal Datasets – large databases containing personal information about a wide range of people – to identify individuals in the course of investigations, to establish links, and as a means of verifying information obtained through other sources. These datasets are an increasingly important investigative tool for the Agencies. The Intelligence Services Act 1994 and the Security Service Act 1989 provide the legal authority for the acquisition and use of Bulk Personal Datasets. However, this is implicit rather than explicit. In the interests of transparency, we consider that this capability should be clearly acknowledged and put on a specific statutory footing.	The Government shares the ISC's conclusion that Bulk Personal Datasets are an increasingly important investigative tool for the Agencies. Part 7 of the draft Bill provides explicit statutory safeguards governing the Agencies' acquisition and use of Bulk Personal Datasets. These include a warrantry regime with an authorisation process that is consistent with other bulk capabilities in the draft Bill.

Y	The Intelligence Services Commissioner currently has responsibility for overseeing the Agencies' acquisition, use and destruction of Bulk Personal Datasets. This is currently on a non-statutory basis. Given that this capability may be highly intrusive and impacts upon large numbers of people, it is essential that it is tightly regulated. The Commissioner's role in this regard must therefore be put on a statutory footing.	The government agrees that wherever possible, oversight should be on a statutory basis. That is why, In an immediate response to the ISC's report, the Prime Minister issued a direction to the Intelligence Services Commissioner putting onto a statutory basis his oversight of the Agencies' acquisition, use, retention and destruction of Bulk Personal Datasets. The proposed new Investigatory Powers Commissioner will have a clear remit to oversee the use of all of the powers available to the security and intelligence agencies, including those relating to Bulk Personal Datasets (see clause 169(3)(a)).
CC	The Agencies may undertake IT Operations against computers or networks in order to obtain intelligence. These are currently categorised as 'Interference with Property' and authorised under the same procedure. Given the growth in, and intrusiveness of, such work we believe consideration should be given to creating a specific authorisation regime.	The Government accepts the ISC's recommendation. Part 5 of the Bill provides a bespoke statutory framework for the ability of the Security and Intelligence Agencies, Armed Forces and law enforcement agencies to undertake equipment interference to obtain communications and other private information and imposes strong safeguards that reflect the interception regime (though not in respect of prohibiting the use of product from equipment interference in criminal trials).
FF	In relation to the activities that we have considered thus far, those which are most intrusive are authorised by a Secretary of State. Some witnesses questioned whether Ministers had sufficient time and independence and suggested that the public had lost trust and confidence in elected politicians to make those decisions. The Committee recognises these concerns. However, one aspect which we found compelling is that Ministers are able to take into account the wider context of each warrant application and the risks involved, whereas judges can only decide whether a warrant application is legally	The Government shares the ISC's view that it is important that Ministers continue to be able to authorise the use of investigatory powers. The Bill preserves the ability of Ministers to make decisions about the necessity and proportionality of a particular warrant and, in doing so, take account of the wider context and risks involved. The Bill also recognises the need to provide further reassurance that these warrants are subject to robust scrutiny and independent oversight. That is why the draft Bill also includes a new provision for a judicial commissioner to approve warrants before they come

	compliant. This additional hurdle would be lost if responsibility were to be transferred to judges and may indeed result in more warrant applications being authorised.	into force. The Government feels that this new 'double lock' provides the right balance between the need for executive oversight and accountability and the need to have a robust authorisation process appropriate to the degree of potential intrusion brought about by each type of warrant.
GG	In addition, Ministers are democratically accountable for their decisions. It is therefore right that responsibility for authorising warrants for intrusive activities remains with them. It is Ministers, not judges, who should (and do) justify their decisions to the public. (We consider later the need for greater transparency: the more information the public and Parliament have, the more Ministers will be held to account.)	
HH	Intrusive capabilities which fall below the threshold requiring a warrant are authorised by officials within the relevant Agency or department. While this is appropriate, there should always be a clear line of separation within the Agencies between investigative teams who request approval for a particular activity, and those within the Agency who authorise it. Further, those capabilities that are authorised by officials should be subject to greater retrospective review by the Commissioners to ensure that these capabilities are being authorised appropriately and compensate for the lack of individual Ministerial Authorisation in these areas.	The draft Bill provides that an authorising officer within a public authority may only authorise the acquisition of communications data where they are independent of the relevant operation (clause 47). There is an exemption for national security purposes. The use of these capabilities will be subject to robust independent oversight by the Investigatory Powers Commissioner.

II	The Commissioners' responsibilities have increased as the Agencies' capabilities have developed. However, this has been piecemeal and as a result a number of these responsibilities are currently being carried out on a non-statutory basis. This is unsatisfactory and inappropriate (as the Commissioners themselves recognise). The Commissioners' non-statutory functions must be put on a clear statutory footing.	The Government accepts the need to enhance the already strong oversight regime. Part 8 of the draft Bill creates a new role of Investigatory Powers Commissioner, who will have the ability to inspect and oversee any aspect of the use of investigatory powers that he or she deems appropriate. The Prime Minister will retain the ability to give statutory directions to the Commissioner to inspect or oversee particular aspects of the agencies' work.
JJ	Throughout this Report, we have recommended an increased role for the Commissioners – in particular, where capabilities are authorised at official level. While this would require additional resources, it would mean that the Commissioners could look at a much larger sample of authorisations.	The Government accepts the ISC's recommendation. The Investigatory Powers Commissioner, provided for in Part 8 of the draft Bill, will have a considerable staff, including inspectors and technical experts. The Commissioner will have the ability to draw on independent expert legal advice as necessary.
KK	While oversight systems in other countries include an Inspector General function, we note that Inspectors General often provide more of an internal audit function, operating within the Agencies themselves. As such, the Committee does not accept the case for transferring to this system: it is important to maintain the external audit function that the Commissioners provide.	The Government agrees that it is important to maintain the external audit function that the current Interception of Communications Commissioner, the Intelligence Services Commissioner and the Chief Surveillance Commissioner provide. The draft Bill creates a new office of The Investigatory Powers Commissioner which will provide independent and more visible scrutiny of the agencies and their work (clause 167).
LL	The Investigatory Powers Tribunal is an important component of the accountability structure. However, we recognise the importance of a domestic right of appeal and recommend that this is addressed in any new legislation.	The Government has accepted the ISC's recommendation and the draft Bill provides a domestic route of appeal from the IPT to the Court of Appeal on a point of law (clause 180).
NN	We are reassured that the Human Rights Act 1998 acts as a constraint on all the Agencies' activities. However, this safeguard is not evident to the public since it is not set out explicitly in relation to each intrusive power. The interactions between the different pieces of legislation which relate to the statutory functions of the intelligence and security Agencies are absurdly complicated, and are not easy for the public to	The Government welcomes the ISC's conclusion that the principles set out in the Human Rights Act 1998 underpin and act as an appropriate constraint all of the activities of the Security and Intelligence Agencies. The draft Bill provides a comprehensive and comprehensible framework governing the acquisition of private communications by the state. All of those powers will be subject to extensive human rights safeguards.

	understand (we address the requirement for a clearer legal framework later in this chapter).	
OO	Section 7 of the Intelligence Services Act 1994 allows for a Secretary of State to sign an authorisation which removes civil and criminal liability for activity undertaken outside the British Islands which may otherwise be unlawful under UK law. We have examined the Class Authorisations allowed under ISA in detail and are satisfied that they are required in order to allow the Agencies to conduct essential work. Nevertheless, that may involve intruding into an individual's private life, and consideration should therefore be given to greater transparency around the number and nature of Section 7 Authorisations.	The draft Bill provides a comprehensive basis for all of the powers available to interfere with private communications, including the use of equipment interference to obtain stored communications (currently authorised under the Intelligence Services Act 1994) (provided at Part 5). The Bill does not provide for interference with equipment for purposes other than the acquisition of communications and other private data. All equipment interference under the Bill must be authorised by a warrant, which will require the Agencies to provide details of the operational purposes or a description of the targets of the warrant as appropriate (clauses 81 to 94). The warrants will be renewable every six months.
PP	We consider that Ministers must be given greater detail as to what operations are carried out under each Class Authorisation: a full list should be provided every six months. We also recommend that Ministers provide clear instructions as to what operations they would expect to be specifically consulted on, even if legally no further authorisation would be required.	
QQ	Under the Intelligence Services Act 1994 and Security Service Act 1989, the Agencies are legally authorised to seek intelligence from foreign partners. However, there are currently no legal or regulatory constraints governing how this is achieved.	The Government considers it vital to be able to share intelligence with foreign partners. We work closely with our allies to prevent terrorist attacks and to stop serious and organised criminals from causing harm. Safeguards already exist that govern the sharing of

RR	We have explored in detail the arrangements by which GCHQ obtain raw intercept material from overseas partners. We are satisfied that, as a matter of both policy and practice, GCHQ would only seek such material on individuals whom they themselves are intercepting – therefore there would always be a RIPA warrant in place already.	intelligence material. The draft Interception of Communications Code of Practice includes specific details on the sharing of intercept material. The draft Bill creates a new role of Investigatory Powers Commissioner, who will have the ability to inspect and oversee any aspect of the use of investigatory powers that he or she deems appropriate, including arrangements for sharing material with foreign partners.
SS	We recognise that GCHQ have gone above and beyond what is required in the legislation. Nevertheless, it is unsatisfactory that these arrangements are implemented as a matter of policy and practice only. Future legislation should clearly require the Agencies to have an interception warrant in place before seeking communications from a foreign partner.	
TT	The safeguards that apply to the exchange of raw intercept material with international partners do not necessarily apply to other intelligence exchanges, such as analysed intelligence reports. While the 'gateway' provisions of the Intelligence Services Act and the Security Service Act do allow for this, we consider that future legislation must define this more explicitly and, as set out above, define the powers and constraints governing such exchanges.	

UU	The Committee does not believe that sensitive professions should automatically have immunity when it comes to the interception of communications. However, some specific professions may justify heightened protection. While the Agencies all operate internal safeguards, we consider that statutory protection should be considered (although we acknowledge that it may be difficult to define certain professions).	The Government agrees that it is important that the use of investigatory powers respects the privilege that attaches to certain communications. The draft Bill will not hinder the ability of lawyers and doctors to do their jobs and protect the privacy of their clients and patients. The Bill – and accompanying codes of practice – will provide strong protections for sensitive professions. Codes of practice will underpin all of the powers in the draft Bill and will be required to include provision relating to the safeguards that apply in respect of sensitive professions and privileged material. The draft Bill also makes explicit provision for additional protections in respect of communications to or from certain sensitive professions. Clauses 16 and 85 of the draft Bill introduces a new statutory requirement for a Secretary of State to consult the Prime Minister before issuing a targeted interception warrant, targeted equipment interference warrant or a targeted examination warrant, where it is intended to intercept or examine the communications of a Member of Parliament or other specified legislative member. In addition, the Government recognises that communications data requests intended to identify journalistic sources should attract additional safeguards beyond authorisation at official level. The Communications Data Code of Practice currently requires public authorities to seek judicial authorisation before obtaining communications data to identify a journalistic source. Clause 61 of the draft Bill puts this requirement onto a statutory footing.

VV	Given the nature of current threats to the UK, the use of Directions under the Telecommunications Act is a legitimate capability for the Agencies. However, the current arrangements in the Telecommunications Act 1984 lack clarity and transparency, and must be reformed. This capability must be clearly set out in law, including the safeguards governing its use and statutory oversight arrangements.	The Government accepts the ISC's conclusion and has included provisions in Part 6 of the draft Bill for the acquisition of communications data in bulk, to put this capability on a more transparent footing, with strengthened safeguards. Strict safeguards are already in place, including regular Secretary of State review of whether the capability continues to be necessary and proportionate. For more than 10 years, successive governments have authorised this critical capability. In a similar way to warrants, Secretaries of States authorise the continued use of Directions on a 6 monthly basis and they are overseen by the Intelligence Services Commissioner. The capability has provided fast and secure access to communications data so that the Agencies can join the dots in their investigations. The draft Bill strengthens these safeguards even further. The power will become subject to the 'double-lock' safeguard of Ministerial and Judicial authorisation and the data is only accessible for specified Operational Purposes. A bulk communications data warrant will have to meet the following test: there must be a national security justification for acquiring the data, it must be necessary and proportionate, and both a Secretary of State and a Judicial Commissioner must approve it. Warrants will last for six months, subject to renewal. Access to data on a day-to-day basis will be strictly controlled and subject to internal justification on grounds of necessity and proportionality. The new Investigatory Powers Commissioner – a senior judge – will provide oversight of the use of this capability.

		Clause 188 of the Bill provides a power for the Secretary of State to issue a national security notice requiring an operator to take necessary steps in the interest of national security. The type of support that may be required includes the provision of services or facilities which would help the intelligence agencies in safeguarding the security of their personnel and operations, or in providing assistance with an emergency (as defined in the Civil Contingencies Act 2004). The Bill makes clear that a national security notice cannot be used for the primary purpose of interfering with privacy, obtaining communications or data. In any circumstance where a notice would involve interference with privacy or the acquisition of communications or data as its main aim, an additional warrant or authorisation provided for elsewhere in the Bill would always be required. As such, a notice of itself does not authorise an intrusion into an individual's privacy.
WW	While our previous recommendations relate to the changes that would be required to the existing legislative framework, the evidence that we have seen suggests that a more fundamental review is now overdue.	The introduction of the draft Bill illustrates the Governments acceptance of the ISC's recommendation. The draft Bill provides a comprehensive and comprehensible framework governing the acquisition of private communications by the state.

YY	The new legislation should clearly list each intrusive capability available to the Agencies (including those powers which are currently authorised under the implicit authorities contained in the Intelligence Services Act and the Security Service Act) and, for each, specify: a. The purposes for which the intrusive power can be used (one or more of: the protection of national security, the safeguarding of the economic well-being of the UK, or the detection or prevention of serious crime). b. The overarching human rights obligations which constrain its use. c. Whether the capability may be used in pursuit of a specific person, location or target, or in relation to a wider search to discover unknown threats. d. The authorisation procedures that must be followed, including the review, inspection and oversight regime. e. Specific safeguards for certain individuals or categories of information – for example, UK nationals, legally privileged information, medical information etc. (This should include incidental collection where it could not reasonably have been foreseen that these categories of information or individuals might be affected.) f. Retention periods, storage and destruction arrangements for any information obtained.	The Government acknowledges the need to ensure that the public are able to understand the laws governing when and how the security and intelligence agencies and law enforcement are allowed to obtain and use their information. The draft Bill provides a clear and comprehensible framework that clarifies which powers different agencies can use and for what purpose. It specifies: - The purposes for which each power may be used and the statutory tests that must be satisfied before a power can be used. - The safeguards that apply to each of the powers, including consideration of wider human rights obligations. - Whether powers must be directed at an individual or a specific operation, or whether they may be used to acquire data in bulk for target discovery purposes. - The authorisations process that applies to each power, reflecting the sensitivity and intrusiveness of that power. - The Codes of Practice that must be laid in respect of each power and which will set out specific safeguards for sensitive professions and privileged material. - The retention, storage and destruction safeguards that apply to material obtained under each of the powers, including, where appropriate, provision through Codes of Practice. - The offences that will apply to unauthorised use of powers and capabilities, including the offence of unlawful

	g. The circumstances (including the constraints that might apply) in which any intelligence obtained from that capability may be shared with intelligence, law enforcement or other bodies in the UK, or with overseas partners. h. The offence which would be committed by Agency personnel abusing that capability. i. The transparency and reporting requirements.	interception and wilful and reckless acquisition of communications data without lawful authority. - The role of the Investigatory Powers Commissioner in overseeing the use of those powers and ensuring appropriate levels of transparency to aid public understanding.

ZZ	In terms of the authorisation procedure, the following principles should apply: a. The most intrusive activities must always be authorised by a Secretary of State. b. When considering whether to authorise the activity, the Secretary of State must take into account, first, legal compliance and, if this is met, then the wider public interest. c. All authorisations must include a summary of the expected collateral intrusion, including an estimate of the numbers of innocent people who may be impacted, and the extent to which the privacy of those innocent people will be intruded upon. d. Any capability or operation which would result in significant collateral intrusion must be authorised by a Secretary of State. e. All authorisations must be time limited (usually for no longer than six months). f. Where an authorisation covers classes of activity conducted overseas, this must include the requirements for recording individual operations conducted under those authorisations, and the criteria for seeking separate Ministerial approval. g. Where intelligence is sought from overseas partners, the same authorisation must be obtained as if the	The draft Bill provides for enhanced authorisation arrangements, including: - Strict legal tests that must be satisfied before authorising a particular activity or imposing an obligation on a communications service provider. - A requirement to take into account collateral intrusion arising as a result of a particular interference. - A strict time limit on each authorisation (ordinarily six months, subject to renewal or review)

	intrusive activity was undertaken by the UK Agency itself. h. Where unsolicited material is received, the circumstances in which it may be temporarily held and assessed, and the arrangements for obtaining retrospective authority (or where authority is not given, destruction of the material) must be explicitly defined.	

AAA	In relation to communications, given the controversy and confusion around access to Communications Data, we believe that the legislation should clearly define the following terms: - 'Communications Data' should be restricted to basic information about a communication, rather than data which would reveal a person's habits, preferences or lifestyle choices. This should be limited to basic information such as identifiers (email address, telephone number, username, IP address), dates, times, approximate location, and subscriber information. - 'Communications Data Plus' would include a more detailed class of information which could reveal private information about a person's habits, preferences or lifestyle choices, such as websites visited. Such data is more intrusive and therefore should attract greater safeguards. - 'Content-Derived Information' would include all information which the Agencies are able to generate from a communication by analysing or processing the content. This would continue to be treated as content in the legislation.	The draft Bill includes revised definitions of the categories of communications data (clause 193): - Entity data will include data about persons or devices, such as subscriber or billing information. - Event data will include data about interaction between persons or devices, such as the fact of a call between two individuals. Before making a request for communications data, public authorities will need to consider which data type they require access to and whether it is necessary and proportionate to do so. Due to the potentially higher level of intrusion associated with Event data, its acquisition must be authorised at a more senior level within the police or other public authorities. Separate safeguards will apply to the acquisition of Related Communications Data (including that derived from content) which may be obtained as a result of bulk interception.

BBB	The Committee has identified a number of areas where we believe there is scope for the Government to be more transparent about the work of the Agencies. The first step – as previously set out – is to consolidate the relevant legislation and avow all of the Agencies' intrusive capabilities. This will, in itself, be a significant step towards greater transparency. Where it is not practicable to specify the detail of certain arrangements in legislation, the Government must nevertheless publish information as to how these arrangements will work (for example, in Codes of Practice). We recognise that much of the detail regarding the Agencies' capabilities must be kept secret. There is, however, a great deal that can be discussed publicly and we believe that the time has come for much greater openness and transparency regarding the Agencies' work.	This draft Bill provides more detail than ever before about the powers available to the agencies, how they are authorised, and the safeguards that apply to them. It will be underpinned by detailed statutory codes of practice. The Investigatory Powers Commissioner will play a visible, independent role in overseeing the work of the agencies and ensuring there is appropriate transparency and public understanding of how they work.

Annex F2

The table below provides an overview of how the Government has responded to the recommendations and conclusions in the report of the Investigatory Powers Review conducted by David Anderson QC.

1	RIPA Part I, DRIPA 2014 and Part 3 of CTSA 2015 should be replaced by a comprehensive new law, drafted from scratch, which: (a) affirms the privacy of communications; (b) prohibits interference with them by public authorities, save on terms specified; and (c) provides judicial, regulatory and parliamentary mechanisms for authorisation, audit and oversight of such interferences.	On enactment, the Investigatory Powers Bill will repeal Part 1 of RIPA and the entirety of DRIPA (and the corresponding amendments made by the CTSA). It also repeals section 94 of the Telecommunications Act 1984 (directions in the interests of national security) and Part 11 of the Anti-Terrorism, Crime and Security Act 2001 (retention of communications data). Part 1 of the Bill asserts the privacy of communications and provides for related offences of unlawful interception or acquisition of communications data. The Bill introduces judicial approval, following the Secretary of State's decision, for the use of interception and equipment interference powers as well as the issue of all bulk warrants, so that there is a 'double-lock' authorisation on the use of these powers. Part 8 of the Bill provides for the creation of a new, more visible oversight body – led by the Investigatory Powers Commissioner (IPC), a senior judge with a team of senior judicial commissioners, and the resources and technical support required, to approve and scrutinise the use of investigatory powers.
2	The new law should amend or replace RIPA Part IV. If Recommendation 82 below is adopted, changes will also be needed to Police Act 1997 Part III, RIPA Parts II and III and RIP(S)A.	Part IV of RIPA will be substantially amended due to the introduction of the Investigatory Powers Commissioner and the creation of a domestic route of appeal from the IPT. The Investigatory Powers Commissioner will have responsibility for the oversight (and in some cases authorisation) of powers exercised under Part III of the Police Act 1997, Parts II and III of RIPA and RIP(S)A.

3	The new law should be written so far as possible in non-technical language.	The Bill has been drafted in so far as possible to be technologically neutral in language. The technical terms that remain in the draft Bill are included to ensure the provisions in the Bill are clear in their intent and application; they are explained in fact sheets and Explanatory Notes published alongside the draft Bill.
4	The new law should be structured and expressed so as to enable its essentials to be understood by intelligent readers across the world.	The Investigatory Powers Bill brings all of the existing powers available to law enforcement and the security and intelligence agencies to obtain communications and data about communications into once piece of legislation, setting out more clearly than ever before what investigatory powers are available to the state, exactly which public authorities are allowed to acquire, access and retain data and under what safeguards and authorisation. It is intended that the public should be able to understand clearly the law governing access and use of their information.
5	The new law should cover all essential features, leaving details of implementation and technical application to codes of practice to be laid before Parliament and to guidance which should be unpublished only to the extent necessary for reasons of national security.	The Investigatory Powers Bill brings the existing law governing the acquisition of communications and communications data into one single piece of legislation. The Bill makes provision for Parliament to approve statutory Codes of Practice that will govern the use of the powers in the Bill. These will cover: Interception of communications Communications data (retention and acquisition) Bulk acquisition of communications data Equipment interference Bulk Personal Datasets
6	The following should be brought into the new law and/or made subject to equivalent conditions to those recommended here	
6a	(a) the general power under section 94 of the Telecommunications Act 1984, so far as it relates to	Paragraph 1 of Schedule 9 to the Bill will repeal section 94 of the Telecommunications Act 1984. Chapter 2 of Part 6 covers the

	matters covered by this Review (cf. ISC Report, Recommendation VV)	acquisition of communications data in bulk, which had previously been provided for under section 94 of the 1984 Act. Clause 188 provides for other capabilities that have been provided for under the 1984 Act by allowing the Secretary of State to issue a notice to a telecommunications operator requiring them to provide assistance in the interests of national security. The new power is subject to strict safeguards, including a prohibition on notices being authorised where the primary purpose is to obtain communications or communications data.
6b	(b) equipment interference (or CNE) pursuant to sections 5 and 7 of the Intelligence Services Act 1994, so far as it is conducted for the purpose of obtaining electronic communications (cf. ISC Report, Recommendations MM-PP);	Equipment Interference (EI) is currently authorised under sections 5 and 7 of the Intelligence Services Act 1994 and part 3 of the Police Act 1997. The use of EI powers will in future be authorised under Part 5 of the Investigatory Powers Bill. This reflects the recommendations of David Anderson QC and the Intelligence and Security Committee of Parliament. A warrant under Part 5 must be sought whenever an agency intends to undertake EI where there is a connection to the British Islands. This applies, as suggested, only to EI conducted with the intention to obtain communications and/or other information. Other EI conduct will continue to be authorised by the relevant current legislation. The IP Bill provides appropriate safeguards for Equipment Interference, reflecting other investigatory powers such as interception. Equipment Interference will be subject to a 'double lock', requiring all EI warrants to be approved by a Judicial Commissioner before they come into force.
6c	(c) interception pursuant to sections 48 and 49 of the Wireless Telegraphy Act 2006 (cf. ISC Report, Recommendations XX-ZZ)	Clause 192 of the Bill amends the Wireless Telegraph Act 2006 so that interception currently authorised under that Act will instead need to be authorised under Part 2 of the draft Bill. Clause 36 authorises

		interception by OFCOM in order to maintain the security of the radio frequency network.
6d	(d) the acquisition and use of bulk personal data (cf. ISC Report, Recommendation X).	A BPD is essentially a description of a category of information and can be obtained through a wide variety of means. We therefore do not consider there is a need for the IP Bill to provide for a power to acquire BPDs; instead they are obtained using the general statutory gateways in the Security Service Act 1989 and the Intelligence Services Act 1994 that the intelligence agencies use for acquiring information. However, Part 7 of the Bill provides for robust and transparent safeguards around BPDs, including a requirement for warrants to authorise the obtaining, retention and examination of BPDs. Those safeguards are comparable to those provided for in relation to other powers under the Bill.
7	The new law should repeal or prohibit the use of any other powers providing for interference with communications. But for the avoidance of doubt, no recommendations are made in relation to the use of court orders to access stored communications (e.g. PACE s9) or the searching of devices lawfully seized, save that it is recommended that oversight should be extended to the former (Recommendation 92(d) below).	Part 1 of the Investigatory Powers Bill makes it an offence to obtain stored communications without lawful authorisation. The obtaining of such communications may be authorised by an interception warrant issued under Part 2 of the Bill or an equipment interference warrant issued under Part 5, which will be subject to IPC oversight. Clauses 10 and 11 of the Bill prohibit authorisations under the Police Act 1997 or the Intelligence Services Act 1994 from authorising the covert acquisition of stored communications from computers in the UK. As now, other statutes may also authorise the overt acquisition of stored communications. Those powers are already subject to a judicial decision (i.e. court orders) or an existing right of appeal (e.g. Schedule 7). The powers to acquire stored communications provided for the in the IP Bill will be overseen by the Investigatory Powers Commissioner.
8	The new law should define as clearly as possible the powers and safeguards governing:	
8a	(a) the receipt of intercepted material and communications data from international partners; and	Schedule 6 of the Bill requires that Codes of Practice issued under the Bill must contain provision about requests to overseas partners for

		intercepted material or related communications data and the handling of material received. Clause 179 provides for the creation of codes of practice. Existing safeguards are set out in the current Interception of Communications Code of Practice.
8b	(b) the sharing of intercepted material and communications data with international partners; (Recommendations 76-78 below).	Safeguards relating to the disclosure of material overseas are provided in clauses 40 and 41 (and 117 and 118 for bulk). Further information about these safeguards will be included in the Interception of Communications Code of Practice. The Bill includes separate provisions which deal with mutual legal assistance (these are set out in clauses 28 and 39 of the Bill).
9	Existing and future intrusive capabilities within the scope of this Review that are used or that it is proposed be used should be (cf. ISC Report, Recommendation BBB): (a) promptly avowed to the Secretary of State and to ISIC; (b) publicly avowed by the Secretary of State at the earliest opportunity consistent with the demands of national security; and, in any event; (c) used only if provided for in statute and/or a Code of Practice in a manner that is sufficiently accessible and foreseeable to give an adequate indication of the circumstances in which, and the conditions on which, communications may be accessed by public authorities.	The Investigatory Powers Bill places all of the powers available to the state to obtain communications and communications data on a clear statutory footing. Relevant Secretaries of State and oversight bodies already have visibility of existing intrusive capabilities and will continue to do so for future such capabilities. The Home Secretary's statement to Parliament on 4 November avowed the use of section 94 of the Telecommunications Act 1984 to acquire communications data in bulk. As demonstrated by the IP Bill and the publication of the Transparency report and reports by the oversight Commissioners and the Intelligence and Security Committee, the Government is committed to enhancing transparency; the Government agrees that we should seek to keep the public as informed as possible consistent with the demands of national security. All activities of law enforcement, the security and intelligence agencies and other public authorities must be in accordance with the law. The Human Rights Act 1998 means all laws must be compliant with Article 8 (right to respect for privacy and family life) of the European Convention on Human Rights with regard to the foreseeability of their use by public authorities to interfere with privacy and with regard to the

		safeguards against abuse. The Government is committed to compliance with those requirements.
10	Within the constraints imposed by national security, the current restrictions and prohibitions relating to the disclosure of warrants and intercepted material (RIPA ss15 and 19, Official Secrets Act 1989 s4) should be clarified and reviewed (cf. ISC Report, Recommendation C) in order to ensure, in particular, that: (a) there is no legal obstacle to explaining the uses (and utility) of warrants to Parliament, courts and public, and that (b) as recommended by the Police Ombudsman for Northern Ireland in his report of 30 October 2014 on the Omagh bombing, there is "absolute clarity as to how specific aspects of intelligence can be shared in order to assist in the investigation of crime".	Clause 43(5)(h) allows for the disclosure of information which does not relate to any specific warrant but relates to interception warrants in general. This will allow the uses and utility of warrants to be explained to Parliament, the courts and the public. Clause 40 imposes restrictions on the access to and disclosure of intercept material, limiting this to the minimum necessary for the authorised purposes. The authorised purposes include the prevention or detection of serious crime. This clause, in combination with s19 of the Counter-Terrorism Act 2008 (which includes provisions on the disclosure of information by the Intelligence Agencies) permits intelligence to be shared with law enforcement bodies in order to assist in the investigation of a serious crime.
11	Breach of Codes of Practice should not automatically constitute a criminal offence: any new criminal offence or enhanced penalty (cf. JCDCDB Report paras 227 and 229; ISC Report, Recommendation T) should be specifically identified in the new law.	A new offence has been created under clause 8 of the Bill of knowingly or reckless obtaining communications data without authority. Other offences are all specified in the draft Bill.

12	The definitions of content and of communications data, and any subdivisions, should be reviewed, with input from all interested parties including service providers, technical experts and NGOs, so as to ensure that they properly reflect both current and anticipated technological developments and the privacy interests attaching to different categories of material and data. Content and communications data should continue to be distinguished from one other, and their scope should be clearly delineated in law.	The Government accepts that there is a need to clarify the different types of communications data. Clause 193 of the draft Bill includes revised definitions of the categories of communications data: - Entity data will include data about persons or devices, such as subscriber or billing information. - Event data will include data about interaction between persons or devices, such as the fact of a call between two individuals. Recognising the more intrusive nature of events data, Schedule 4 of the draft Bill requires the acquisition of event data to be authorised at a more senior level than entity data. CSPs and technical experts were consulted in the development of the definitions in the Bill and proposals were shared with NGOs at an early stage. The Government will continue to invite views on the definitions before a revised Bill is introduced to Parliament in 2016.
13	ATCSA 2001 Part 11 should be repealed, and the voluntary code of practice issued under it should be withdrawn.	Part 1 of Schedule 9 The Investigatory Powers Bill repeals ATCSA 2001 Part 11
14	The Home Secretary should be able by Notice (as under DRIPA 2014 s1 and CTSA 2015 s21) to require service providers to retain relevant communications data for periods of up to a year, if the Home Secretary considers that the requirement is necessary and proportionate for purposes laid down in Article 15(1) of the e-Privacy Directive.	This is provided for under Clause 71 of the Bill.

15	In relation to the subject matter of the 2012 Communications Data Bill, Government should initiate an early and intensive dialogue with law enforcement and CSPs in order to formulate an updated and coordinated position, informed by legal and technical advice, on the operational case for adding web logs (or the equivalent for non-web based OTT applications) to the data categories currently specified in the Schedule to the Data Retention Regulations 2014 for the purposes of:	The Government has considered the operational case for the provisions in the 2012 draft Communications Data Bill. Following consultation with law enforcement and communications service providers, we consider that there is a strong operational case for providing for the retention of internet connection records, which will indicate the specific internet services to which a person or device has connected. The Government recognises the sensitive nature of internet connection records and for that reason clause 47 restricts the purposes for which they can be acquired further than other forms of communications data. A designated senior officer in a public authority will only be able to require disclosure or processing of internet connections records for the following purposes: - To identify the sender of an online communication. This will often be in the form of an IP address resolution and the internet service used must be known in advance of the application - To identify which communication services a person has been using. For example whether they are communicating through apps on their phone - To identify where a person has accessed illegal content. For example an internet service hosting child abuse imagery. Clause 71 of the draft Bill also provides that local authorities will not be permitted to acquire internet connection records under any circumstances.

		Before making a request for communications data, public authorities will need to consider which data type they require access to and whether it is necessary and proportionate to do so.
a	(a) resolving shared IP addresses or other identifiers (in particular, to identify the user of a website);	Clause 47 restricts the purposes for which internet connection records can be acquired consistent with this. The retention of ICRs is necessary in order to resolve IP addresses consistently
b	(b) identifying when a person has communicated through a particular online service provider (so as to enable further enquiries to be pursued in relation to that provider); and/or	Clause 47 restricts the purposes for which internet connection records can be acquired consistent with this. We consider there is a strong case for allowing law enforcement to access ICRs for this purpose. The case for access to ICRs for this and other purposes has been published alongside the draft Investigatory Powers Bill.
c	(c) allowing websites visited by a person to be identified (to investigate possible criminal activity)	Clause 47 restricts this purpose to establishing whether a person is accessing or making available material the possession of which is a crime (e.g. to identify whether a person had uploaded illegal images to a website). We consider there is a strong case for allowing law enforcement to access ICRs for this purpose. The case for access to ICRs for this and other purposes has been published alongside the draft Investigatory Powers Bill.

d	Full consideration should be given to alternative means of achieving those purposes, including existing powers, and to the categories of data that should be required to be retained, which should be minimally intrusive. If a sufficiently compelling operational case has been made out, a rigorous assessment should then be conducted of the lawfulness, likely effectiveness, intrusiveness and cost of requiring such data to be retained. No detailed proposal should be put forward until that exercise has been performed.	The Government has engaged intensively with law enforcement agencies to make the operational case for the inclusion of internet connection records. The case has been published alongside the draft Bill.
16	The rules regarding retention of data by CSPs should comply (to the extent that it may be applicable) with EU law as contained e.g. in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and with the ECHR, particularly as regards:	The provisions of DRIPA, with its increased safeguards, together with the robust access regime provided for by RIPA, created a regime that responded to the judgment while still ensuring the system was operationally workable. The judgment of the Divisional Court in the judicial review of DRIPA has been appealed to the Court of Appeal which has decided to make a preliminary reference to the European Court of Justice to clarify the effect of the Digital Rights Ireland judgment.
16 a	(a) limits on the data whose retention may be required;	
16 b	(b) ensuring that retention periods are no longer than necessary;	
16 c	(c) ensuring the protection and security of data and their destruction when the retention period ends; and	
16 d	(d) the location in which data are stored.	
17	To the extent that a requirement is placed on CSPs that may result in them retaining partial or complete web logs or equivalent, the circumstances in which access may be sought by public authorities and the conditions on which access should be granted should be the subject of guidance in a Code of Practice and/or from ISIC, and sufficient records should be kept to allow ISIC to verify	Clause 47 restricts the purposes for which internet connection records can be acquired. Local authorities may not acquire internet connection records at all. There is existing guidance in codes of practice on the retention of and access to CD. New codes are provided for in the Bill (Schedule 6) The current Interception of Communications Commissioner (whom the IPC will replace) provides guidance on acquisition issues to forces and we

	through regular audit and inspection that requests have been properly authorised.	will ensure that appropriate records continue to be kept and that regular audits and inspections continue to take place.
18	There should be no question of progressing proposals for the compulsory retention of third party data before such time as a compelling operational case may have been made, there has been full consultation with CSPs and the various legal and technical issues have been fully bottomed out. None of those conditions is currently satisfied.	The Government has decided that there will be no third party data retention requirements imposed on CSPs. While there would still be operational benefit from the retention of third party data, that benefit has declined as a result of encryption.
19	The capability of the security and intelligence agencies to collect and analyse intercepted material in bulk should be maintained, subject to rulings of the courts, but used only subject to the safeguards in Recommendations 40-49 and 72-80 below, and only in cases where it is necessary to achieve an objective that cannot be achieved by the new and less extensive power in Recommendation 42(b) below.	Part 6, Chapter 1 of the Bill maintains the ability for the security and intelligence agencies to carry out bulk interception. The safeguards mirror those in the targeted interception clauses in Part 2, Chapter 1.
20	In relation to interception and the acquisition of communications data, the following types of compulsory warrant and authorisation should be available:	
20a	(a) For the interception of communications in the course of transmission, · an specific interception warrant · a combined warrant · a bulk interception warrant.	Clause 12(1)(a) provides for the Secretary of State to make a targeted interception warrant, Clause 184 and Schedule 7 of the Bill provide for the combining of warrants and authorisations. Part 6, Chapter 1 provides for the making of Bulk interception warrants by the Secretary of State.

20b	(b) For the acquisition of communications data in bulk, a bulk communications data warrant.	Chapter 2 of Part 6 of the Bill provides for this.
20c	(c) For the acquisition of communications data otherwise than in bulk, an authorisation.	Part 3 of the Bill provides for this.
21	To the extent that Recommendation 6 above is adopted, the analogous activities there referred to should be subject to equivalent procedures.	The Investigatory Powers Bill applies strict safeguards and oversight to the EI regime, reflecting other powers, such as interception – detailed at clause 103. The safeguards and processes cannot be identical, due to the operational differences between the techniques. The key difference between Interception and EI in this regard is the use of the information obtained as evidence in legal proceedings. Equipment interference techniques are currently used by law enforcement agencies to bring criminals to justice, including through the use of EI product in court. The Bill does not change the current approach. This is set out at clause 103(4)(d).
22	Specific interception warrants, combined warrants, bulk interception warrants and bulk communications data warrants should be issued and renewed only on the authority of a Judicial Commissioner.	The Bill introduces a "double-lock" authorisation model which requires that a targeted interception warrant, bulk interception warrant or bulk communications data warrant signed by the Secretary of State must also be approved by a Judicial Commissioner before it can come into force. Authorising warrants is one of the means by which Secretaries of State hold the agencies and the police to account, and in turn, they are accountable to Parliament for how those powers are authorised and exercised. Introducing a judicial element to the authorisation process will ensure both democratic accountability, and independent verification.

		The authorisation process in the case of combined warrants is outlined at Schedule 7. It sets out that regardless of who issues the warrant, where two or more powers are authorised under the same warrant then the authorisation of that warrant will be subject to approval by a Judicial Commissioner.
23	Authorisations for the acquisition of communications data otherwise than in bulk should be issued only on the authority of a Designated Person authorised to do so by the authorising body.	Clause 46 provides for this. (The Bill also provides for collaboration agreements under which public authorities may, or may be require to, collaborate on use of DPs and SPOCs in line with other recommendations.)
24	It is not recommended that service providers wishing to offer services in the UK should be required to have a licence, or that they should be required to store data in the UK. But in order to address deficiencies in access to material from overseas service providers, the Government should:	We agree with this recommendation, and have not legislated in the Bill that service providers wishing to offer services in the UK should be required to have a licence, or that they should be required to store data in the UK.
24a	(a) seek the cooperation of overseas service providers, including by explaining so far as possible the nature of the threat, how requests are authorised and overseen, and the steps that are taken to ensure that they are necessary and proportionate;	We are continuing to engage and work with communications service providers who provide services to users in the UK. Companies that work across international boundaries regularly have to manage competing legal obligations. We will always work with companies to ensure they can meet their obligations under RIPA.
24b	(b) seek the improvement and abbreviation of MLAT procedures, in particular with the US Department of Justice and the Irish authorities; and	The UK has been working closely with counterparts in the US to improve the quality of requests and to streamline processes under the existing bilateral MLAT. The UK has also been speaking to the Irish authorities

		about the extent to which the EU Mutual Legal Assistance Convention might provide for access to data stored in Ireland.
24c	(c) take a lead in developing and negotiating a new international framework for data-sharing among like-minded democratic nations.	This work is underway. Sir Nigel Sheinwald, the PM's special envoy on access to data, discussed with the companies and the US and other governments a solution that would allow certain democratic countries - with similar values and high standards of oversight, transparency and privacy protection - to gain access to content in serious crime and counter-terrorism cases through direct requests to the companies. The Government is now taking this forward. Clause 39 of the Bill provides for companies in the UK to comply with interception requests in accordance with any future relevant international agreement.
25	Pending a satisfactory long-term solution to the problem, extraterritorial application should continue to be asserted in relation to warrants and authorisations (DRIPA 2014 s4), and consideration should be given to extraterritorial enforcement in appropriate cases.	Clauses 29 and 30 provide for the service of interception warrants on persons who provide services to customers in the UK, irrespective of whether the company is based in the UK or not. Clause 31(8) makes clear that the power is enforceable through civil proceedings.
26	Only those currently specified in RIPA s6 should be entitled to apply for a specific interception warrant.	Clause 15 sets out those who may apply for an interception warrant. This is the same position as currently provided for in section 6 of RIPA.
27	Specific interception warrants should be limited to a single person, premises or operation. Where a warrant relates to an operation, each person or premises to which the warrant is to apply, to the extent known at the time of the application, should be individually specified on a schedule to the warrant, together with the selectors (e.g. telephone numbers) applicable to that person or premises.	Clauses 23(3) and(4) of the Bill require that a targeted interception warrant must name or describe the person or organisation and, in relation to an operation, must describe the purpose or activity
28	The only purposes for which a specific interception warrant can be issued should be, as under RIPA s5(3):	

28	(a) preventing or detecting serious crime (including by giving effect to a mutual legal assistance agreement), or	Clause 14(3) sets out the statutory purposes for which an interception warrant can be sought. These are the same as the purposes in section 5 of RIPA.
28	(b) in the interests of national security (including safeguarding the economic well-being of the UK in a respect directly linked to the interests of national security).	
29	29. Applications for interception warrants should contain the following information: (a) The background to the operation or investigation in the context of which the warrant is sought (b) The person(s) or premises to which the application relates, to the extent known at the time of application, and how they feature in the operation (c) A description of the communications to be intercepted, details of the service provider(s) and an assessment of the feasibility of the interception to the extent known at the time of application (d) A description of the conduct to be authorised or the conduct it is necessary to undertake in order to carry out what is authorised or required by the warrant (e) An explanation of why that conduct is considered to be necessary for one or more of the permitted statutory purposes (f) An explanation of why any likely intrusion into privacy is proportionate to what is sought to be achieved by that conduct, explaining why less intrusive alternatives have not been or would not be as effective (g) Consideration of any collateral intrusion and why that intrusion is justified in the circumstances (h) Whether the application is made for the purposes of	Clause 23 sets out the requirements that a warrant must satisfy. Further information about detail that should be included in warrant applications will be provided in codes of practice.

	determining matters that are privileged or confidential such as (for example) the identity or a witness or prospective witness being contacted by a lawyer or the identity of or a journalist's confidential source (i) Whether the application relates to a person who is known to be a member of a profession that handles privileged or confidential information (including medical doctors, lawyers, journalists, Members of Parliament or ministers of religion), and if so what protections it is proposed will be applied (j) Where an application is urgent, the supporting justification (k) An assurance that all material intercepted will be kept for no longer than necessary in accordance with the applicable rules, and handled in accordance with the applicable procedures for minimisation, secure holding and destruction.	
30	When a specific interception warrant is sought for the purpose specified in Recommendation 28(b) above (national security) and that purpose relates to the defence of the UK and/or the foreign policy of the Government, the Secretary of State should have the power to certify that the warrant is required in the interests of the defence and/or foreign policy of the United Kingdom. In such cases, the Judicial Commissioner in determining whether to issue the warrant (Recommendation 31 below) should be able to depart from that certificate only on the basis of the principles applicable in judicial review.	The 'double lock' authorisation regime applies to all warrants issued under the Bill. This will preserve democratic accountability and introduce a further element of independent verification.

31	3A specific interception warrant should be issued only if it is established to the satisfaction of a Judicial Commissioner that:	Under the provisions in the Bill, warrants will only be authorised by the Secretary of State where they are necessary and proportionate for a permitted statutory purpose and where the conduct is lawful. A Judicial Commissioner will then review the Secretary of State's decision, applying judicial review principles. This will include considering whether the use of investigatory powers is necessary and proportionate. The Commissioner would also determine whether the use of the powers would be lawful. If the Judicial Commissioner disagreed with the decision of the Secretary of State under our proposed model, the warrant would not come into force.
31a	(a) the warrant is necessary for one or both of the permitted statutory purposes (Recommendation 28 above);	
31b	(b) the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct; and	
31c	the assurances regarding the handling, retention, use and destruction of the intercepted material, including in relation to privileged or confidential material, are satisfactory.	Clause 14 requires the Secretary of State to be satisfied that these safeguards are in place before authorising a warrant.
32	Arrangements should be put in place for the prompt consideration of urgent applications for specific interception warrants from any part of the UK and at any time.	Clause 20 of the Bill provides that if a warrant is deemed by a Secretary of State to be urgent, then it will come in to force immediately. It will then last for five working days and must be reviewed by a Judicial Commissioner during this time.
33	Should an application for a specific interception warrant be rejected, the Judicial Commissioner should give reasons for rejection. In the event of rejection, the applicant for a warrant should be able to:	Clause 19 provides that if the Judicial Commissioner disagreed with the decision of the Secretary of State, the warrant would not come into force. In that case, the Judicial Commissioner must provide written reasons for the refusal. The Bill provides an 'appeal' mechanism by which the Secretary of State may ask the Investigatory Powers Commissioner to reconsider the warrant, but the IPC's decision would be final. There is no means by which a Secretary of State could overrule a Commissioner.
33a	(a) re-submit an amended application, addressing the defects or omissions identified by the Judicial Commissioner; or	
33b	(b) request a final ruling on the original application from the Chief Judicial Commissioner, by way of appeal from the original rejection.	

33c	(c) The Chief Judicial Commissioner may consider any such appeal in conjunction with one or more other Judicial Commissioners.	
34	It should normally be for a Judicial Commissioner to make major modifications to a specific interception warrant, e.g. the addition of a new person or premises to the schedule. So far as applicable, the information listed at Recommendation 29 above should be supplied and considered before such a modification is authorised. However, a Judicial Commissioner should have the power to authorise a DP meeting the requirements set out in Recommendations 56 and 57 below to make major modifications to a specific interception warrant on the basis that such modifications are then notified promptly to the Judicial Commissioner. The circumstances in which this could be appropriate should be specified in a Code of Practice and might include, for example, (1) urgent or fast moving cases, and (2) cases in which the interference with privacy is always likely to be small, or to be consistent across possible targets.	Clause 26 of the Bill provides that a major modification can be made by: the Secretary of State; a member of the Scottish Government; or a senior official acting on behalf of the Secretary of State or a member of the Scottish Government. The Investigatory Powers Commissioner may retrospectively scrutinise any modifications made to a warrant.
35	Provision should be made for minor modifications (e.g. the addition of a new telephone number for an existing target) to be made, after consideration of the implications if any for privacy, collateral intrusion and proportionality, by a DP meeting the requirements set out in Recommendations 56 and 57 below.	Clause 26 provides that a minor modification can be made by: the Secretary of State; a member of the Scottish Government; a senior official acting on behalf of the Secretary of State or a member of the Scottish Government; a senior person in a warrant requesting department, the person to whom the warrant is addressed or another senior official in the warrant requesting department.
36	A Judicial Commissioner should have the power to cancel a specific interception warrant at any time, if it appears to the Judicial Commissioner that one or more of the conditions for its issue are no longer satisfied.	The Secretary of State will have an obligation to cancel any warrant that no longer meets the conditions of its issue. The Investigatory Powers Commissioner will provide retrospective oversight of this process and all

		aspects of the warrantry regime. Judicial Commissioners will formally consider warrants that the point of their issue and renewal.
37	Specific interception warrants should have a duration of six months. The Judicial Commissioner who issues the warrant should have a discretion to require that it be reviewed by a Judicial Commissioner at a specified time before its expiry.	Clause 24 makes clear that targeted interception warrants will last six months except in urgent cases, in which they will last only five days. As is currently the case, the Secretary of State will have the ability to attach conditions to the approval of warrants (which might include a requirement for an update to be submitted to the Secretary of State before the sixth month period).
38	Warrant renewals should take effect from the date of expiry of the warrant (as currently under RIPA Part I Chapter 2) rather than from the date of renewal (as currently under RIPA Part I Chapter 1).	Clause 24(2)(b) provides for this.
39	Combined warrants should be subject to the same rules as interception warrants, save that:	Clause 184 and Schedule 7 of the Bill provide that certain warrants can be combined for purposes of operational efficiency. All combined warrants must include either an EI or interception warrant and so all combined warrants will be subject to the double lock authorisation procedure. A combined warrant allows the Secretary of State and/or Judicial Commissioner who is authorising the warrant to look across the full range of actions that may be applied to the subject of the warrant. This allows them to take a more informed decision about the necessity and proportionality of the action being undertaken. It is also more efficient for the agency applying for the warrant.
39a	(a) They may authorise, in the context of a given operation, more than one of (1) interception, (2) intrusive surveillance and (3) property interference.	
39b	(b) They must explain why the conditions for each type of warrant are satisfied, and why it is necessary and proportionate for a combined warrant to be issued.	
40	Only the Director General of MI5, the Chief of MI6 and the Director of GCHQ, in each case with the approval of the Secretary of State, should be eligible to apply for bulk warrants.	Part 6 provides that only the security and intelligence agencies can apply for a bulk warrant.

41	The restrictions in Recommendation 27 should not apply to bulk warrants.	This is reflected in the bulk warrant provisions at Part 6 of the Bill.
42	There should be two types of bulk warrant:	
42a	bulk interception warrants, which would allow content and related communications data to be obtained; and	Clause 106 provides for this.
42b	bulk communications data warrants, which would allow only communications data to be obtained.	Clause 122 provides for this.
42c	A bulk interception warrant should never be applied for, approved or authorised in circumstances where a bulk communications data warrant would suffice.	Clause 107 requires the Secretary of State to consider whether it is necessary to acquire content under a bulk interception warrant, or whether it is sufficient to obtain related communications data under that warrant.
43	The purposes for which a bulk warrant is sought should be:	This is provided for at clauses 107, 122 and 137 of the Bill. The Secretary of State and Judicial Commissioner must authorise the operational purposes which will govern when material collected in bulk can be selected for examination, at the same time as they authorise its acquisition.
43a	(a) limited to the permitted statutory purposes (Recommendation 28 above);	
43b	(b) (in lieu of the certificate provided for by RIPA s8(4)(b)), limited to one or more specific operations or mission purposes (e.g. “attack planning by ISIL in Iraq/Syria against the UK”).	
44	Bulk interception warrants should, in addition, be required to be targeted at the recovery of intercepted material comprising the communications of persons believed to be outside the UK at the time of those communications. It should be determined (if Recommendation 42(b) is adopted) whether an analogous restriction is necessary or desirable in relation to bulk communications data warrants.	Clause 106 specifies that a bulk interception warrant may only be issued where the main purpose is for the interception of overseas related communications. The Bill does not impose an analogous restriction for the acquisition of communications data in bulk. The power to acquire domestic communication data currently allows the security and intelligence agencies to make vital investigative connections in order to understand terrorist networks and to disrupt threats in the UK. The Bill puts this power on a clearer statutory footing and makes it subject to equivalent safeguards to other bulk powers.

45	Applications for bulk warrants should contain the following information: a) The specific operation(s) or mission purpose(s) in respect of which they are sought (b) Description of the communications to be intercepted or acquired, details of the CSP(s) and an assessment of the feasibility of the interception or acquisition (c) Description of the conduct to be authorised, or the conduct it is necessary to undertake in order to carry out what is authorised or required by the warrant (d) A statement specifying both the statutory purpose(s) and, as precisely as possible, the operations or mission purposes in relation to which material is sought (e) An explanation, backed by evidence, of why the interception or acquisition is considered to be necessary for one or more of the permitted statutory purposes and for the operations or mission purposes identified (f) An explanation of why any likely intrusion into privacy is proportionate to what is sought to be achieved by that conduct, explaining why less intrusive alternatives have not been or would not be as effective (g) Consideration of any collateral intrusion and why that intrusion is justified in the circumstances (h) Whether the application could result in acquisition of material or data that is privileged or confidential material, and if so what protections it is proposed will be applied	Clauses 106, 122 and 135 set out the information that must be included in bulk warrant applications. Clauses 111, 125, 140 require bulk warrants to specify the operational purposes for which any intercepted material or related communications data may be selected for examination. Further detail about the contents of warrant applications will be included in codes of practice issued under the Bill.

	(i) In the case of a bulk interception warrant, an explanation of why a bulk communications data warrant would not be an adequate alternative (j) In the case of a bulk communications data warrant, an explanation of why an authorisation would not be an adequate alternative (k) Where an application is urgent, supporting justification (l) Details of the use that it is proposed to make of the data that is recovered, including in relation to possible sharing and use in combination with other datasets. (m) An assurance that all material recovered will be retained no longer than necessary, looked at, used or analysed only for certified purposes and in accordance with the applicable rules, and handled in accordance with the applicable procedures for minimisation, secure holding and destruction.	
46	46. When approving a bulk warrant that is sought in whole or in part for the purpose referred to in Recommendation 28(b) above (national security), and when that purpose relates to the defence of the UK and/or the foreign policy of the Government, the Secretary of State should certify: (a) that the warrant is required in the interests of the defence and/or foreign policy of the United Kingdom; and (b) that it is required for the operation(s) and/or mission purpose(s) identified.	The 'double lock' authorisation regime applies to all warrants issued under the Bill. This will preserve democratic accountability and introduce a further element of independent verification.

47	In such cases, the Judicial Commissioner in determining whether to issue the warrant (Recommendation 48 below) may depart from that certificate only on the basis of the principles applicable in judicial review.	The 'double lock' authorisation regime applies to all warrants issued under the Bill. This will preserve democratic accountability and introduce a further element of independent verification.
48	A bulk warrant should be issued only if it is established to the satisfaction of a Judicial Commissioner that: (a) its purpose and targets are limited by reference to the factors identified in Recommendations 43 and 44 above; (b) it is necessary for one or more of the permitted statutory purposes; (c) it is necessary for the mission purpose(s) and/or operation(s) identified; (d) in the case of a bulk interception warrant, it is necessary for the warrant to apply to content as well as communications data; (e) the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct; and that (f) the assurances regarding the handling, retention, use and destruction of the intercepted material or acquired data, including in relation to privileged or confidential material, are satisfactory.	The 'double lock' authorisation regime applies to all warrants issued under the Bill. This will preserve democratic accountability and introduce a further element of independent verification.
49	Recommendations 32-38 above should apply also to bulk warrants, save that any modification to a bulk warrant must be authorised by a Judicial Commissioner.	Part 6 of the Bill includes relevant provisions.
50	Public authorities with relevant criminal enforcement powers should in principle be able to acquire communications data. It should not be assumed that the public interest is served by reducing the number of	The Government has reviewed the public authorities with communications data powers. 13 public authorities were removed from RIPA last year. Otherwise the list of public authorities included in the Bill that can acquire communications data has been subject to minimal

	bodies with such powers, unless there are bodies which have no use for them. There should be a mechanism for removing public authorities (or categories of public authorities) which no longer need the powers, and for adding those who need them.	change. Schedule 4 of the Bill lists all public authorities that will have powers under Part 3 of the Bill.
51	The issue of which (if any) categories of communications data should be unavailable to certain public authorities should be reviewed, in the light of Recommendation 12 above and any revision of procedures for authorisation and review. (Some examples of the potential value to local authorities of what is currently known as traffic data are at Annex 16 to this report.)	Schedule 4 of the Bill provides that all public authorities should have access to all data reflecting their requirements with the exception of local authorities who are prohibited from acquiring internet connection records. The Bill includes a power to add or remove public authorities.
52	The grounds on which communications data may be acquired should remain as set out in RIPA s22(2), subject to any limitation (relating, for example, to the need for crime to exceed a certain threshold of seriousness, which would not necessarily need to be set at the same level as in RIPA s81(2)(b)) that may be required by EU law or the ECHR.	Clause 46 sets out the purposes for which communications data can be acquired in the Bill. They remain the same as in RIPA.
53	Communications data should be acquired only after the grant by a designated person (DP) of an authorisation. Details of the authorisation should be served on a CSP where it appears to the DP that the CSP is or may be in possession of, or capable of obtaining, any communications data. The distinction between an authorisation and a notice (RIPA s22) is unnecessary and should be abandoned.	Clause 46 provides for the substance of this recommendation. Under the provisions in the Bill, a designated senior officer will issue an authorisation. That authorisation authorises engaging in conduct to acquire communications data. Where appropriate, that may include the issue of a notice to a CSP requiring the disclosure of CD.
54	The application for an authorisation should set out the matters specified in the Acquisition and Disclosure of	Schedule 6 of the Bill provides for statutory Codes of Practice, which will provide further detail about applications.

	Communications Data Code of Practice (March 2015) 3.5-3.6.	
55	An authorisation should be granted only if the DP is satisfied, having taken the advice of the SPoC and considered all the matters specified in the application, that it is necessary and proportionate to do so.	Clauses 46 (authorisations) and 60 (requirement to consult a Single Point of Contact) provide for this.
56	DPs should be persons of the requisite rank or position with the requesting public authority or another public authority. The Regulation of Investigatory Powers (Communications Data) Order 2010 should be revised after consultation in the light of: (a) Recommendation 12 above; (b) the comments of IOCCO (December 2014 submission to the Review, 3.3) on the appropriate rank of DPs and the need for consistency across public authorities and in relation to comparable methods of surveillance; and (c) The new functions placed on DPs and summarised at Recommendations 59(b) and 60 below.	Clause 54 with Schedule 4 provide for this.
57	DPs should be adequately trained in human rights principles and legislation (including in relation to privileged or confidential material), and may grant authorisations only when and to the extent that it is necessary and proportionate to do so in the specific circumstances.	Schedule 6 provides that a Code of Practice may contain provision about the training of people exercising functions under the Bill. The communications data code, to which regard must be had when exercising functions, must also make provision about privileged or confidential material. The assessment of necessity and proportionality under clause 46 will include the specific circumstances of the case.

58	As recently stated in the ISC Report, Recommendation HH: "there should always be a clear line of separation within the Agencies between investigative teams who request approval for a particular activity, and those within the Agency who authorise it". DPs (including in the security and intelligence agencies) should be required by statute to be independent from operations and investigations when granting authorisations related to those operations and investigations, and this requirement should be implemented in a manner consistent with the ECHR and EU law.	Clause 47 provides for the independence of the DSO with exceptions for specified exceptional circumstances (eg, in the interests of national security) and smaller public authorities that have insufficient staff.
59	The function of DPs should be: (a) To authorise the acquisition of communications data (Recommendation 55 above); (b) To make references to ISIC on applications for privileged/confidential material and, where appropriate, on novel/contentious applications (Recommendations 68 and 70 below).	Clause 61 provides that requests for communications data for the purpose of identifying or confirming journalistic sources must be approved by a judicial commissioner. The Code of Practice will provide that the IPC must be consulted about novel and contentious requests for communications data.
60	In addition, DPs appointed by the nine bodies entitled to intercept communications data should be entitled to authorise minor modifications to specific interception warrants (Recommendation 35 above).	Clause 26 provides that a minor modification can be made by: the Secretary of State; a member of the Scottish Government; a senior official acting on behalf of the Secretary of State or a member of the Scottish Government; or a senior person in a warrant requesting department.
61	No authorisation should be granted (save in exceptional circumstances specified in the new law) without the prior opinion of an accredited Single Point of Contact (SPoC). The purpose of the SPoC should be: (a) to ensure that only practical and lawful requirements for communications data are undertaken; and	Clause 60 provides for this.

	(b) to facilitate the lawful acquisition of communications data, and effective co-operation between a public authority and CSPs.	
62	The functions of the SPoC should be set out in statute along the lines of the March 2015 Code of Practice on the Acquisition and Disclosure of Communications Data, para 3.22.	Clause 60 sets out the functions of a SPoC.
63	SPoCs should not have to be located within the requesting authority. For example, there would be no obstacle to police SPoCs being organised on a regional or national level, as is the National Anti-Fraud Network (NAFN).	Clauses 62 and 64 provides for collaboration agreements between police and other public authorities, which may include the sharing of SPoCs and designated officers between authorities.
64	In the case of local authorities, the SPoC function should continue to be compulsorily performed through a SPoC at NAFN.	Clause 58 requires local authorities to be in collaboration agreements. In practice this will mean that they must use the SPoCs at NAFN.
65	In the case of the other "minor users", responsible between them for less than 1% of requests for communications data in 2014, the SPoC function should in future also be compulsorily performed by a SPoC at NAFN, which will need to be resourced for that purpose.	Clauses 62 and 63 provide for voluntary and compulsory collaboration agreements which provide for sharing of SPOC as well as DSO functions. This provides flexibility about who smaller public authorities should collaborate with.
66	The requirement in RIPA 2000 ss23A-B of judicial approval by a magistrate or sheriff for local authority requests for communications data should be abandoned. Approvals should be granted, after consultation with NAFN, by a designated person of appropriate seniority within the requesting public authority.	In order to provide reassurance about the use of communications data by local authorities, clause 59 provides for judicial authorisation of local authority applications for communications data. This responsibility will continue to be undertaken by magistrates.

67	When the communications data sought relates to a person who is known to be a member of a profession that handles privileged or confidential information (including medical doctors, lawyers, journalists, Members of Parliament or ministers of religion), the new law should provide for the DP to ensure that (1) special consideration is given to the possible consequences for the exercise of rights and freedoms, (2) appropriate arrangements are in place for the use of the data, and (3) the application is flagged for the attention of ISIC inspectors.	Schedule 6 of the Bill requires that the statutory Codes of Practice deal with these issues
68	If communications data is sought for the purposes of determining matters that are privileged or confidential such as (for example) (1) the identity or a witness or prospective witness being contacted by a lawyer or (2) the identity of or a journalist's confidential source, the DP should be obliged either to refuse the request or to refer the matter to ISIC for a Judicial Commissioner to decide whether to authorise the request.	Clause 61 provides for judicial commissioner approval of requests for communications data to identify or confirm journalistic sources.
69	A Code of Practice, and/or ISIC guidance, should specify (1) the rare circumstances in which it may be acceptable to seek communications data for such a purpose, and (2) the circumstances in which such requests should be referred to ISIC.	The Bill provides that such decisions must be authorised by a Judicial Commissioner. The communications data Codes of Practice issued under Schedule 6 will provide further detail.
70	In recognition of the capacity of modern communications data to produce insights of a highly personal nature, where a novel or contentious request for communications data is made, the DP should refer the matter to ISIC for a Judicial Commissioner to decide whether to authorise the request.	A Code of Practice issued under the Bill will provide that Judicial Commissioners' advice should be sought in where a novel and contentious request for communications data is made.

71	A Code of Practice, and/or ISIC guidance, should specify the circumstances in which such requests should be referred to ISIC.	
72	Safeguards at least equivalent to those in RIPA s15, as elaborated in section 7 of the Interception of Communications draft Code of Practice, should ensure that the domestic disclosure, dissemination, copying, storage and retention of intercepted material is limited to the minimum necessary for the authorised purposes.	Clauses 40-42 provide for safeguards replicating those in sections 15 and 16 of RIPA. The relevant provisions in the draft Interception of Communications Code of Practice under RIPA will be reflected in the new code issued under the Bill.
73	Equivalent statutory safeguards should be provided in relation to communications data. In particular, the new law and a Code of Practice issued under it, with the involvement of the Information Commissioner as appropriate, should make provision for: (a) why, how and where data are retained within public authorities; (b) who may access them within the public authority; (c) with whom the data may be shared, and under what conditions; (d) the special rules needed as regards the treatment of data that appear to be privileged or confidential (see Recommendations 67-69 above), and data relating to a victim or a witness; (e) the processing of data for reasons going beyond their acquisition; (f) the use of data in conjunction with other datasets; (g) the processes for determining which data should be destroyed or further retained; and (h) compliance with the Data Protection Act 1998.	Paragraph 3 of Schedule 6 specifically requires the Acquisition of CD Code of Practice to include provision on these matters

74	These safeguards should be enforced and backed up by ISIC audits (as currently performed by IOCCO), examining: (a) how the material and/or data were used or analysed; (b) whether they were used for the stated or intended purpose; (c) what actual interference or intrusion resulted, and whether it was proportionate to the aim set out in the original authorisation; (d) whether the conduct became disproportionate to what was foreseen at the point of authorisation, and if so whether the operational team initiated the withdrawal of the authorisation; (e) retention, storage and destruction arrangements; and (f) whether any errors or breaches resulted from the interference or intrusion.	The IPC will oversee all aspects of access to communications data under the Bill
75	On the basis that MI5, MI6 and GCHQ each apply the safeguards referred to in Recommendations 72-73 above, they should be permitted to share intercepted material and communications data between them for the purposes of their respective functions.	As now, the security and intelligence agencies will continue to be able to share intercepted material and communications data for the purposes of their respective functions.
76	Any receipt of intercepted material or communications data from third countries should be on the basis of clearly-defined safeguards, published save insofar as is necessary for the purposes of national security and monitored by ISIC, including a warrant governing any intercepted material that is sought (ISC Report, Recommendations QQ-TT).	Schedule 6 of the Bill requires that codes of practice issued under the Bill must contain provision about requests to overseas partners for intercepted material or related communications data and the handling of material received. Clause 179 provides for the creation of codes of practice. Existing safeguards are set out in the current Interception Code of Practice.

77	Any transfer of intercepted material or communications data to third countries should be on the basis of clearly-defined safeguards, published save insofar as is necessary for the purposes of national security and monitored by ISIC.	Safeguards relating to the disclosure of intercepted material overseas are provided in clauses 40 and 41. Further information about these safeguards will be included in the Interception of Communications Code of Practice. The Bill includes separate provisions which deal with mutual legal assistance (these are set out in clauses 28 and 39 of the Bill). Paragraph 3 of Schedule 6 specifically requires the Acquisition of CD Code of Practice to include provision on these matters
78	The new law should make it clear that neither receipt nor transfer as referred to in Recommendations 76-77 above should ever be permitted or practised for the purpose of circumventing safeguards on the use of such material in the UK.	Intercepting agencies will be bound by the obligations at clauses 40 and 41 and by further restrictions set out in codes of practice. Their compliance will be overseen by the Investigatory Powers Commissioner.
79	Content that is acquired pursuant to a bulk interception warrant and that relates to a communication involving a person believed to be in the UK should be made available to be read, looked at or listened to only on the basis of a specific interception warrant issued by a Judicial Commissioner (Recommendations 26-38 above): cf. in part ISC Report, Recommendations Q and R.	Clause 119 places a prohibition on selecting intercepted material for examination if any criteria used for the selection of that material refer to an individual known to be in the UK and are aimed at identifying the content of communications sent by or intended for that individual. If the intercepting agencies wish to examine the communications of a person believed to be in the UK that have been collected in bulk, a targeted examination warrant must be sought (provided for in Clause 12).
80	The new law should in addition provide for appropriately rigorous and rights-compliant procedures for the purposes of authorising access to:	
80a	(a) content that is acquired pursuant to a bulk warrant and that does not relate to a communication involving a person believed to be in the UK; and	This is provided for by clauses 117-119.

80b	(b) (if Recommendation 42(b) is adopted), communications data that are obtained pursuant to a bulk warrant.	Safeguards for communications data obtained under a bulk acquisition warrant are set out in clauses 131-132. Safeguards for related communications data obtained under a bulk interception warrant are set out in clause 117-119. This includes additional provisions as related communications data obtained via interception is subject to an evidential bar.
81	The bar in RIPA s17 on using intercepted material as evidence in legal proceedings (recently endorsed after lengthy consideration in Cm 8989) did not form part of this Review. Consideration should however be given to adding to the list of exceptions in RIPA s18, without prejudice to any other possible additions, proceedings before (1) the Parole Commissioners for Northern Ireland and (2) the Sentence Review Commissioners in Northern Ireland.	Paragraph 13 of schedule 3 provides for this.
82	The Interception of Communications Commissioner's Office (IOCCO), the Office of Surveillance Commissioners (OSC) and the Intelligence Services Commissioner (IsCommr) (the current Commissioners) should be replaced by a new Independent Surveillance and Intelligence Commission (ISIC).	Part 8 of the Bill provides for these functions to be subsumed by the Investigatory Powers Commissioner.
83	It should be the duty of every relevant person to disclose or provide to ISIC all such documents and information as ISIC may require for carrying out its functions, as is the case for the current Commissioners under RIPAs s58 and 60 and the Police Act 1997 s107(5)(a).	Clause 175 provides for this.
84	ISIC (through its Judicial Commissioners: see Recommendations 106-107 below) should be granted powers:	

84a	(a) to issue and renew warrants (Recommendation 22 above);	The 'double lock' authorisation regime applies to all warrants issued under the Bill. This will preserve democratic accountability and introduce a further element of independent verification.
84b	(b) to make major modifications to specific interception warrants and combined warrants (Recommendations 34 and 39 above);	
84c	(c) to make modifications to bulk warrants (Recommendation 49 above);	
84d	(d) to cancel warrants that it has issued (Recommendations 36, 39 and 49 above);	
84e	(e) to authorise applications for communications data referred to it by public authorities pursuant to Recommendations 68 (privileged and confidential material) and 70 (novel and contentious) above; and	Judicial Commissioners will have the power to authorise requests for communications data to identify journalistic sources (clause 61). Codes of Practice will specify circumstances in which public authorities must seek advice in novel and contentious cases.
84f	(f) to issue guidance (cf. the OSC's Procedures and Guidance of December 2014) to public authorities in relation to issues arising in relation to applications for warrants and the grant of authorisations, which would supplement the new law and any codes of practice issued under it and which should be published where the constraints of national security permit.	Clause 172 provides for this.
85	The functions referred to in Recommendation 84 above should only be performed by Judicial Commissioners who hold or have held high judicial office (High Court or above), subject to the possibility of delegating certain functions to persons who hold or have held judicial office at least at the level of Circuit Judge. As currently with the OSC, the judicial authorisation function should be independent from and in no sense subordinate to the other functions of ISIC.	Clause 169 provides for this. Judicial Commissioners will be required to hold or have held high judicial office.

86	Judicial Commissioners should use their power where appropriate to request further clarification, information or documents from the requesting public authority, and/or to consult standing counsel on any point of legal difficulty. Public authorities should have a right of appeal to the Chief Judicial Commissioner (Recommendation 33(b) above).	Clause 19(5) provides for public authorities to appeal a decision of a Judicial Commissioner to the Investigatory Powers Commissioner. Judicial Commissioners will be able to seek any further factual clarifications that they feel necessary and may use some of their increased resources to appoint legal counsel.
87	ISIC (through its Judicial Commissioners) should also take over from the OSC its equivalent functions (in relation to public authorities other than the security and intelligence agencies) in relation to intrusive surveillance, property interference and undercover officers under RIPA Part II, RIP(S)A and the Police Act 1997.	Clauses 178, 169 and 173 provide for this.
88	ISIC should be resourced so as to enable it to provide a prompt, efficient and reliable warrantry service in all jurisdictions of the United Kingdom.	Clause 176 provides for this by dealing with funding for the Investigatory Powers Commissioner.
89	The existing audit and inspection functions of the current Commissioners should be transferred to the ISIC, including: (a) all those set out in RIPA Parts I-III, RIP(S)A and the Police Act 1997, to the extent that they are consistent with the arrangements in the new law; (b) the audit of the use by security and intelligence agencies of their holdings of Bulk Personal Datasets (cf. ISC Report, Recommendations X and Y); and (c) the recently granted power to oversee the operation of directions under Telecommunications Act 1984 s94 (IOCCO Report, March 2015, section 10), to the	Clauses 178, 169 and 173 provide for this.

	extent that such power may survive the introduction of the new law.	
90	ISIC should have the power to review compliance with the terms of any warrant, authorisation or guidance that may have been issued by the Judicial Commissioners. Where error is found, an Inspector should be able to recommend that the warrant in question be reviewed by a Judicial Commissioner with a view to its possible modification or cancellation.	The Investigatory Powers Commissioner will be able to review all activity relating to the use of investigatory powers covered by warrants (Clause 169). If a serious error is found then the Investigatory Powers Commissioner may refer the matter to the Investigatory Powers Tribunal as per clause 171.
91	In addition, ISIC should have the power to inspect: (a) The exercise by DPs of all the functions summarised in Recommendations 59 and 60 above (b) The treatment by public authorities of privileged and confidential material (c) The retention, storage, processing and destruction of all communications data acquired by public authorities (not just, as currently for IOCCO, communications data only when it is related to intercepted material) (d) The use of such data, including in combination with other datasets (cf. ISC Report, Recommendation Y) (e) The use by public authorities of open-source intelligence (OSINT)	Clause 169 provides for this.

	(f) The sharing of intercepted material and communications data within the UK Government (g) The receipt of intercepted material and communications data from, and the transfer of such material and data to, foreign governments (Recommendations 76-78 above).	
92	Additional gaps in the arrangements relating to IOCCO's current activities (explained in IOCCO's submission of December 2014 to this Review) should be filled when ISIC is constituted. In particular:	
92a	(a) Express provision should be made for error reporting, and for a procedure for arriving at and keeping under review the definition of an error where interception is concerned.	Clause 171 provides for this.
92b	(b) There should be a statutory requirement for ISIC to review the giving of notices by the Secretary of State (currently under DRIPA 2014 s1) requiring the retention of specific communications data by a CSP.	Clause 169 provides for this.
92c	(c) ISIC should have the power to report on refusals by service providers (including overseas service providers, given the extraterritorial effect of the law) to intercept communications or disclose communications data when a lawful request is made of them.	Clause 174 provides for the Investigatory Powers Commissioner to report upon any matter relating to investigatory powers in their annual or other reports.

92d	(d) There should be statutory provision for oversight of the operation of powers for interception and/or obtaining communications data other than in the new law, to the extent that such powers survive, including the power to access stored data by order of the court under PACE s9.	Clause 169 provides for the Investigatory Powers Commissioner to be able to review all covert activity relating to the use of investigatory powers under the Bill, but not court orders.
93	Though strictly outside the scope of this Review, it would also be appropriate to review the existing powers of the OSC and of the ISCommr so as to identify any other gaps that should be filled when constituting the ISIC.	The Investigatory Powers Commissioner will be able to review all activity relating to the use of investigatory powers (Clause 169).
94	ISIC (like IOCCO before it) should have the capacity to inspect the work of analysts, investigators, SPoCs and DPs on live cases as well as on cases that are closed.	The Investigatory Powers Commissioner will be able to review all covert activity relating to the use of investigatory powers (Clause 169).
95	ISIC should have the power to report on, to issue guidance on and to participate in the preparation of Codes of Practice any activity which it has the power to inspect.	The Investigatory Powers Commissioner may issue a report on any area or subject relating to the work of the Investigatory Powers Commissioner that they feel is necessary (clause 174(5)). He or she may also provide assistance and guidance to public authorities and others as per clause 172(2).
96	96. ISIC should inherit the intelligence oversight functions of the ISCommr, including:	Clauses 178,169 and 173 provide for this.
96a	(a) oversight of the Consolidated Guidance to Intelligence Officers and Service Personnel; and	Clauses 178,169 and 173 provide for this.
96b	(b) keeping under review the activities of the Agencies or others engaging in intelligence activity, as directed by the Prime Minister under RIPA s59A.	Clause 170 provides for this.
97	Consideration could be given to granting ISIC a more general supervisory power over the activities of the Agencies, but subject to Recommendation 118 (no duplication of functions and resources).	The Investigatory Powers Commissioner will be able to review all activity relating to the use of investigatory powers (Clause 169) as well as the existing functions of the Intelligence Services Commissioner.

98	ISIC should be subject to the same obligation as the current Commissioners (RIPA s68(2)) to provide assistance to the IPT, and should be kept informed of proceedings relevant to its functions (as by RIPA s68(3)).	This is provided for in clause 172(1).
99	ISIC should further be given the power, on its own initiative or at the suggestion of a public authority or CSP, and subject to a duty not to disclose anything that would be damaging to national security or prejudice ongoing operations, to: (a) and (b) in any case in which in the opinion of ISIC it is possible that the scale or nature of the error might entitle the subject of the error to compensation.	
99a	(a) inform a subject of an error on the part of a public authority or CSP; and	The Investigatory Powers Commissioner will be able to inform a subject of an error (clause 171(1)) Subject to meeting the conditions included in clause 171(2) that are that the error is sufficiently serious and the IPT judge that the impact on the individual is such that it is in the public interest for the individual to be informed.
99b	(b) inform the subject of his right to lodge an application to the IPT.	Clause 171(8)(a) provides for this.
100	To the extent that Recommendation 6 is adopted, the powers and functions set out in Recommendations 84-99 above should apply in an equivalent manner to the activities there referred to.	Clause 169 provides for this.
101	There should be a report at least once in every year dealing with all aspects of the work of ISIC, and supplemented as may be feasible by more regular statistical releases.	Clause 174 provides for this.
102	As an expert, apolitical body with a strong judicial ethos, ISIC should also have the power to carry out inquiries and produce reports into matters falling within its remit,	The Investigatory Powers Commissioner may look at any issue within their remit of investigatory powers. The Prime Minister has also direct the Commissioner to inspect/ carry out particular inquiries (clause 174).

	at the request of the Prime Minister or on its own initiative.	
103	The Prime Minister should have the power to redact ISIC's annual report on narrowly specified grounds (cf. RIPA s58(7)). The Prime Minister should be obliged to lay ISIC's annual report before Parliament within a certain number of days (or sitting days) of receipt.	Clause 174 provides for this.
104	The Chief Commissioner should be a person of unquestioned professional distinction and independence, committed not only to leading the work of ISIC but to accounting publicly and to Parliament for that work, and to building public awareness of ISIC and its role. The Chief Judicial Commissioner should be eligible to serve also as Chief Commissioner, but need not necessarily do so: some possibilities are illustrated in the diagrams at Annexes 17-18 to this Report.	The Investigatory Powers Commissioner will be a powerful, visible new role and will be expected to build public and Parliamentary awareness of his work.
105	The Chief Commissioner should be appointed by the Prime Minister. Consideration should be given to allowing the ISC a voice in the appointment or confirmation of the Chief Commissioner.	This is provided for by clause 167.
106	Judges entitled to authorise warrants should be known as Judicial Commissioners (or Assistant Judicial Commissioners) so as to emphasise their distinct and independent status. There should be regular dialogue and sharing of experience between the Judicial Commissioners and the inspectorate.	Judicial Commissioners will review Secretary of State decisions to approve investigatory powers warrants on Judicial Review principles. Judicial Commissioners will also have a role to play in determining what should happen to any material that was gathered under an urgent warrant that was later quashed by a Judicial Commissioner.

107	Judicial Commissioners could be full-time or (as currently in the OSC) part-time judges on duty according to a rota. They should be capable of providing prompt and efficient service for applications from all parts of the United Kingdom. It will be necessary to provide 24-hour cover (as currently by the Secretary of State) for cases where urgent applications for warrants and authorisations arise out of hours.	The IPC will provide 24-hour cover to deal with urgent authorisations. The Bill also provides an urgency procedure where a Secretary of State issued warrant can take effect without prior Judicial Commissioner approval.
108	An inspectorate should be provided for the audit and inspection functions entrusted to ISIC.	The IPC will have a large body of technical inspectors to advise them in their functions.
109	ISIC should have staff with the necessary expertise (including technical expertise) and resources in relation to: (a) each power whose operation it audits or inspects (including interception and encryption, communications data, directed and intrusive surveillance, property interference and CHIS/undercover); and (b) each function relating to intercepted material and data (including acquisition, use, storage, retention, dissemination, sharing and destruction).	The IPC will have a large body of technical inspectors, in house legal advisors and communications support. In addition to this the Commissioner will have a budget provision to buy in any additional expertise that they feel is necessary.
110	ISIC should have an in-house legal presence and one or more security-cleared standing counsel, appointed on a part-time basis from the independent practising Bar, whose function would be, on request: (a) to give advice on recent developments in the law, (b) to advise ISIC on possible legal vulnerabilities in the arrangements whose operation it reviews; (c) to advise (at the request of the Judicial Commissioners) in relation to applications for warrants	The IPC will have an in house legal presence and a budget provision to spend on external advisors when they feel there services are necessary.

	or requests for authorisations on proposed communications data authorisations; (d) to assist with the legal aspects of formulating guidance and contributing to Codes of Practice; and (e) by these means to help ISIC ensure that the activities it authorises, audits or reviews are lawful, and that the public authorities it oversees have due warning of legal difficulties.	
111	111. Within the necessary constraints of security: (a) ISIC should be public-facing, transparent and open to diverse ideas (including from all sectors of the community in all parts of the UK, from other countries, from international institutions and from young people who have grown up online). (b) It should be willing to draw on expertise from the worlds of intelligence, computer science, technology, academia, law and the NGO sector, and should engage with and support compliance officers and compliance mechanisms within public authorities, DPs and SPoCs. (c) As much as possible of its output (including, within the constraints of national security, any guidance that it may issue) should be published on a user-friendly website. (d) Commissioners and staff should attend and participate in conferences, invite dialogue, assist the conduct of research and be alert to the adoption and dissemination of international best practice. (e) ISIC should make itself accessible to traditional media, and have an active social media presence.	The Government has made clear that it will provide the necessary technical, legal, and communications expertise to enable the IPC to undertake their oversight and authorisation functions effectively. In particular, the Government is keen that the new body more effectively engages the public and Parliament. Exactly how the IPC does this will be a matter for them, given it is an independent body.

112	ISIC should be sufficiently resourced to enable it to perform functions which are more extensive than those performed by the almost 40 full-time and part-time current Commissioners and staff.	The IPC will have a large body of technical inspectors, in house legal advisors and communications support. In addition to this the Commissioner will have a budget provision to buy in any additional expertise that they feel is necessary.
113	The jurisdiction of the IPT should be expanded (or clarified) to cover circumstances where it is a CSP rather than a public authority which was at fault (for example, by intercepting the wrong communications address and/or disclosing the wrong communications data).	The IPT will continue to scrutinise the activities of public authorities. CSPs are already subject to inspection from the Information Commissioner and can be held accountable for any errors that they make through this route.
114	There should be a right of appeal to an appropriate court from rulings of the IPT, on points of law only, permission being required in the normal way from either the IPT or the appellate court (cf. ISC Report, Recommendation LL).	Clause 180 provides for this
115	The IPT (which is chaired by a High Court Judge or Lord Justice of Appeal) should be given the same power as the High Court to make a declaration of incompatibility under HRA 1998 s4, particularly (but not exclusively) should Recommendation 114 not be adopted.	The Government is accepting recommendation 114 and believes that this provides a sufficient right of appeal. The Court of Appeal will be able to make a declaration of incompatibility.
116	The IPT should have the resources it needs to operate in a practical and expeditious manner. Those resources should be independent of those allocated to ISIC and the ISC, whose conduct may from time to time be in issue before the IPT.	The IPC and IPT will have separate resources and they are independent of one another.
117	The IPT should where appropriate require ISIC to provide it with assistance, particularly of an investigative nature, as it has several times required the existing Commissioners to do pursuant to RIPA s68(2).	Clause 172 provides for this.

118	There should continue to be a committee of parliamentarians with oversight of the work of the security and intelligence agencies and trusted by them with classified information, not only because parliamentary oversight is desirable in principle but because of the knowledge and understanding that its members bring to parliamentary debates with national security implications, e.g. in relation to terrorism legislation and proscription orders.	The Intelligence and Security Committee of Parliament will continue to fulfil this role.
119	The functions of ISIC and the ISC should not overlap. In particular, there should be no duplication of reporting functions or resources between the ISC and ISIC.	A Memorandum of Understanding will be developed to minimise overlap between the two bodies.
120	It should be for Parliament to consider whether: (a) to retain the system of Prime Ministerial appointment but require the Chair to be a member of a political party not represented in government; (b) to transfer the ISC's investigative resource in due course to ISIC; and/or (c) to recast the ISC as a Select Committee (either on its own or merged with the Defence Select Committee) whose members would be elected in the normal way, and to which ISIC would report where necessary in closed session.	The nature and role of the ISC was discussed during the passage of the Justice and Security Act 2013. The Investigatory Powers Bill does not include any further suggestions for reforming the role of the ISC. Should Parliament consider that further changes to the Committee are needed then this may be proposed during the passage of the Bill and the Government will consider.
121	It should be recognised that the operation of covert powers is and should remain secret, and that transparency in relation to operational matters is not a realistic goal.	We endorse this observation.

122	Public authorities should however be as open as possible (cf. ISC Report, Recommendation BBB). They should consider how they can better inform Parliament and the public about why they need their powers, how they interpret those powers, the broad ways in which those powers are used and why any additional capabilities might be required. They should contribute to any consultations on the new law, so as to ensure that policy-making is informed by the best evidence.	The Investigatory Powers Bill provides more detail than ever before about the powers available to the agencies, how they are authorised, and the safeguards that apply to them. It will be underpinned by detailed statutory Codes of Practice. The Investigatory Powers Commissioner will play a visible, independent role in overseeing the work of the agencies and ensuring there is appropriate transparency and public understanding of how they work.
123	The statistics provided by ISIC should be as informative as possible: the proposals put forward by IOCCO in its December 2014 submission to this Review provide a useful starting point.	This will be provided for in a Memorandum of Understanding
124	Both ISIC and the IPT should be as open as possible in their work, and should seek actively to make the public aware of their role as a check on the powers of public authorities.	The Government has made clear that it will provide the necessary technical, legal, and communications expertise to enable the IPC and IPT to undertake their functions effectively. Exactly how they engage with the public and Parliament will be a matter for them, given they are independent bodies.

Annex F3

The table below provides an overview of how the Government has responded to the recommendations and conclusions in the Report of the Independent Surveillance Review Panel convened by the Royal United Services Institute.

1	We support the view – as described in both the Intelligence and Security Committee of Parliament (ISC) and Anderson reports – that the current surveillance powers are needed but that they require a new legislative framework and oversight regime. We do not believe that the ISC's recommendation of consolidating all current laws relating to the intelligence agencies in a single legal framework is required to achieve substantial reform, nor do we think there should be separate legislation for the police and for the security and intelligence agencies. We agree with David Anderson's suggestion that RIPA 2000 Part I, DRIPA 2014 and Part 3 of the CTSA 2015 should be replaced by a comprehensive new law.	On enactment, the Investigatory Powers Bill will repeal RIPA 2000 Part 1, and DRIPA 2014 (and the corresponding amendments made by the CTSA 2015). It also repeals Section 94 of the Telecommunications Act 2015 (directions in the interests of national security) and Part 11 of the Anti-Terrorism, Crime and Security Act 2001 (retention of communications data).
2	The new legislation should be clearly articulated while also recognising the complexity of the issues. Codes of Practice, published in statute, should be written in plain and accessible language and include details of implementation and technical application of the legislation.	The new Bill brings the existing law governing the use of investigatory powers into one single piece of legislation. Codes of Practice will be published alongside the Bill. These will cover: • Interception of Communications • Communications data (retention and acquisition) • Bulk acquisition of communications data • Equipment interference • Bulk Personal Datasets

3	Following evidence received by the ISR Panel and further discussion with civil-liberties groups and communications service providers (CSPs), we recommend that definitions of content data and of communications data should be reviewed as part of the drafting of new legislation. They should be clearly delineated in law.	Clause 193 of the draft Bill sets out definitions of communications data and the content of communications in a way that is technologically neutral. Under RIPA communications data is currently broken down into three sub-categories: traffic data, service use information and subscriber information. The Bill replaces the existing definitions as follows: <u>Communications data</u> is categorised into: • Entity data – This data is about entities or links between them but does not include information about individual events. Entities could be individuals, groups and objects (such as mobile phones or other communications devices). • Events data – Events data identifies or describes events which consist of one or more entities engaging in an activity at a specific point, or points, in time. The Bill provides, for the first time, the definition of content. The content of a communication or other item of private information is the data which reveals anything of what might be reasonably be expected to be the meaning of that data, disregarding any meaning that can be inferred from the fact of the communication or the existence of an item of private information. Additionally, Clause 82 creates a further category of data known as Related Communications Data/Equipment data. Communications data and equipment data include communications data and any data which enables or otherwise facilitates the functioning of any system or service provided by the system. It also allows data with the

		characteristics of communications data to be extracted from the content of the communication where the data, once extracted, does not reveal the meaning of the content of the communication.

4	While the number of public authorities with the power to obtain communications data has recently been reduced, we believe (i) that there should be a periodic review of which public bodies have the authorisation to use intrusive powers (such as directed surveillance and interception of communications) and (ii) that all relevant applications from authorised public bodies to obtain communications data must be made via the National Anti-Fraud Network as the national single point of contact in the future.	The Government regularly reviews which authorities have access to communications data. Authorities can only be added through the enhanced affirmative procedure, but they will be able to be removed through the negative procedure. The other powers provided in the Bill (interception and equipment interference) are available to the law enforcement and security and intelligence agencies. Only a small subset of law enforcement agencies have the ability to intercept, and those authorities who can access these powers are listed on the face of the Bill. The ability to collect any data in bulk is limited to the security and intelligence agencies. The investigatory powers provided for in Part 2 of RIPA (directed and intrusive surveillance) are outside the scope of the IP Bill. However, authorities with access to these powers are kept under review. An experienced single point of contact (SPoC) is a crucial safeguard in any application for communications data. Clause 62 of the draft Bill provides for collaboration agreements between authorities where designated senior officers and SPoCs can be shared. These collaboration agreements can be voluntary or there is a power for the Secretary of State to require public authorities to enter it them. The power will be used to ensure minor users of communications data use an experienced SPoC function, such as the National Anti-Fraud Network. It would not be appropriate for all authorities to use NAFN because NAFN do not have the resources or the expertise to make all requests for communications data – such a requirement would increase their communications data work by more than 200 fold.

5	A national approach to policing in the digital era is necessary and long overdue. The police require a unified national digital policing strategy and the resources to deliver the capability to ensure digital investigations and intelligence capability. This will require a co-ordinated national effort bringing the relevant bodies together, and a review of core training in digital investigations and intelligence skills for all officers.	The Government recognises the need for policing to respond to a digitally enabled society. We are supporting police led digital transformation strategies which will develop digital investigation and intelligence capabilities at the local, regional and national level.
6	A Technical Advisory Board was established under RIPA 2000 which brought together industry experts in a personal capacity. Since its inception, the Board has not met regularly and is seen as ineffectual. The government should replace the Board with an Advisory Council for Digital Technology and Engineering. The Advisory Council would be a statutory and non-departmental public body established under new legislation. Terms of reference for a new Advisory Council should be drawn up so as to keep under review the domestic and international situation with respect to the evolution of the Internet, digital technology and infrastructure, as well as: • Provide advice to relevant ministers, departments and agencies on technical measures • Promote co-operation between the public and private sectors • Manage complaints from CSPs on notices and measures they consider unreasonable • Advance public education • Support research on technology and engineering.	Clause 183 provides for a Technical Advisory Board comprising of industry and agency experts to provide advice to the Secretary of State on the cost and technical feasibility of implementing a particular obligation. To date, the TAB has never been required to fulfil its statutory function. However, rather than being indicative of an ineffective Board, it is illustrative of close collaboration between the Home Office and CSPs; and the fact that financial reimbursement arrangements are in place that meet CSPs' requirements. A number of other bodies already exist to bring industry and government together in matters of interception and communications data, such as the Telecommunications Industry Security Advisory Council (TISAC) and the Interception and Communications data Strategy Groups (LISG and CDSG respectively). We therefore judge that the TAB performs an important safeguard for CSPs in their negotiations with government on strategic interception capabilities. In addition, the Investigatory Powers Commissioner which will be established by the Bill will have increased resources, including an

7	The Advisory Council should be a resource for a new National Intelligence and Surveillance Office (see Recommendation 17) and the ISC.	expanded team of technical inspectors, in house legal advisors and a communications expert. The Commissioner will also have a budget to "buy in" any further technical resource that they feel is necessary to fulfil their broad new remit."
8	The capability of the security and intelligence agencies to collect and analyse intercepted material in bulk should be maintained with stronger safeguards as set out in the Anderson Report. In particular, warrants for bulk interception should include much more detail than is the case currently and be the subject of a judicial authorisation process, save for when there is an urgent requirement (see Recommendation 10, point 2).	Part 6 of the Bill provides for the security and intelligence agencies to collect communications and communication data in bulk, putting existing powers onto a clear statutory footing in one piece of legislation. The Bill states that a bulk warrant must specify the operational purposes for which material collected in bulk may be examined by an analyst. The operational purposes must be agreed by the Secretary of State and approved by a Judicial Commissioner as set out in clauses 107 and 109. Before an analyst can access any data obtained under a bulk warrant, he or she will need to ensure that it is necessary and proportionate, and is in accordance with the relevant operational purpose. In addition, analysts will only be able to examine the content of the communications of a person believed to be in the UK if they have obtained a targeted examination warrant which must be issued by the Secretary of State, and approved by a Judicial Commissioner (clause 119).

9	We agree with both the ISC and Anderson reports that there should be different types of warrant for the interception and acquisition of communications and related data, and have drawn on both sets of recommendations. We recommend three types of warrant for the interception of communications and an authorisation for communications data: 1. For the interception of communications in the course of transmission we suggest two different types of warrant: a. A specific interception warrant which should be limited to a single person, premises or operation b. A bulk interception warrant which would allow content data and related communications data to be obtained. 2. For the acquisition of communications data in bulk, a bulk communications data warrant which would be limited to the acquisition of communications data 3. For the acquisition of communications data otherwise than in bulk, an authorisation by the relevant public authority. Communications data should only be acquired after the authorisation is granted by a designated person.	Part 2 of the IP Bill provides for targeted interception warrants, targeted examination warrants (which allows for the examination of data which has collected in bulk that relates to person believed to be in the UK) and mutual assistance warrants. A targeted interception warrant, as set out in clause 12, authorises interception in the course of transmission and of related communications data. These warrants may relate to a particular person or organisation or a single set of premises, which must be named or described in the warrant. It may also related to more than one person, organisation or set of premises where the conduct authorised is for the purpose of the same investigation. This must be described and as many of the entities as is practical must be named on the warrant (clause 23). A bulk interception warrant, as specified in clause 106, is for the purpose of intercepting overseas communications in bulk and also related communications data. The warrant must specify the operational purposes for which the communications and data issued under this warrant may be selected for examination (clause 111). A bulk acquisition warrant, as specified in clause 122, permits the acquisition of communications data in bulk, as defined in clause 193. All bulk warrants must be issued by the Secretary of State and approved by a Judicial Commissioner. The Secretary of State and the Judicial Commissioner also authorise the operational purposes which determine the circumstances in which the material collected in bulk can be selected for examination. The authorisation for the acquisition of communications data other than in bulk, is set out in clause 46. It may only be authorised by a

		designated senior officer at a rank stipulated in Schedule 4 of the Bill. This clearly sets out the relevant officer in each public authority which may authorise the acquisition of communications data. Before granting an authorisation, the designated senior officer is required, by virtue of clause 60, to consult a person acting as a single point of contact (SPoC). The SPoC is an accredited officer, trained to facilitate lawful acquisition between the public authority and the CSP. The SPoC can provide advice to both the officer making the application for communications data and the designated senior officer as to the lawfulness of the request.

10	We recommend that the government adopts a composite approach to the authorisation of warrants, dependent on the purpose for which the warrant is sought and subsequent degree of ministerial input required. Our approach does not discriminate between whether it is law-enforcement or an intelligence agency submitting the warrant. 1. Where a warrant (see points 1a, 1b and 2 in Recommendation 9) is sought for a purpose relating to the detection or prevention of serious and organised crime, the warrant should always be authorised by a judicial commissioner. Most police and other law-enforcement warrants would fall into this category. A copy of each warrant should be provided to the Home Secretary (so that the Home Secretary and officials can periodically examine trends in serious and organised crime, for example). 2. Where a warrant (see points 1a, 1b and 2 in Recommendation 9) is sought for purposes relating to national security (including counter-terrorism, support to military operations, diplomacy and foreign policy) and economic well-being, the warrant should be authorised by the secretary of state subject to judicial review by a judicial commissioner. The review should take place before implementation of the warrant. If there is a case of urgency the secretary of state should be able to direct that a warrant comes into force immediately, and the	Warrants for interception and (for the security and intelligence agencies) equipment interference for all the specified purposes in the Bill (national security, economic well-being and serious crime) will continued to be issued by the Secretary of State as set out in clauses 14 and 107. The Bill does, however, require the warrant to be approved by Judicial Commissioner before it comes into force (clauses 19 and 90). The Judicial Commissioner will apply the principles of judicial review when considering a warrant issued by the Secretary of State. In urgent cases, clauses 20 and 91 make provision for the Secretary of State to issue a warrant without the approval of a Judicial Commissioner, however the Judicial Commissioner must approve the warrant within 5 days of it being issued. If the Judicial Commissioner does not approve the warrant within this period, it ceases to have effect. The Judicial Commissioners will be part of the Investigatory Powers Commission but they will be independent of the arm of the Investigatory Powers Commissioner who will inspect the public authorities' use of investigatory powers. The Commission will perform two distinct functions and will employ two separate teams to complete these functions. The first of these teams will approve the warrant authorising the use of investigatory powers. The second, oversight team will look at how the powers authorised under that warrant were used by the public authority as well as taking a wider system overview of the full process This follows the model of the Office of Surveillance Commissioners who currently authorise LEA use of intrusive surveillance and Covert Human Intelligence Sources and also inspect LEA use of the powers and report their findings to

	judicial commissioner should be notified straight away and the judicial review conducted within fourteen days. The judicial commissioners in charge of the authorisation of warrants should not be part of a new National Intelligence and Surveillance Office nor should they be based in a government department, but alternative office facilities should be sought so that the commissioners are accessible but remain independent. To ensure no loss of operational efficiency, appropriately qualified judges would have to be available at all times throughout the year.	the Prime Minister. They will be based in appropriate offices, independent of Government.

11	The Investigatory Powers Tribunal (IPT) should be as open as possible and proactively find ways that make its business less opaque to the public.	Currently those wishing to challenge a judgment from the IPT must bring it before the European Court of Human Rights (ECtHR). This system can be time consuming, opaque and difficult to understand. In order to increase public confidence that those who use investigatory powers are fully held to account by the law, and that Articles 8 and 10 of the European Convention on Human Rights are respected, we are creating a right to challenge the decisions of the IPT in a higher court within the UK (clause 180). All applications (complaints and claims) will be capable of being subject to an appeal, where there is a substantive point of law at issue.
12	The IPT should hold open public hearings, except where the Tribunal is satisfied that private or closed proceedings are necessary in the interests of justice or other identifiable public interest.	It is already the case that the IPT considers the cases before it in open sessions where it is able to do so. The IPT recognise the need to be transparent about their work and will continue to hold open hearings wherever possible.
13	The IPT should have the ability to test secret evidence put before it by the SIAs. While internal procedures are a matter for the Tribunal to decide, we suggest that this could be achieved through the appointment of a special counsel.	It is already the case that the IPT can test the evidence put before it. In some circumstances, when the IPT deem it necessary, Counsel to the Tribunal is appointed whose role it is to ensure that all parties to the proceedings are represented. The IPT will also be able to draw on the expertise of the Investigatory Powers Commissioner, where appropriate.
14	We agree with both the ISC and Anderson reports that the domestic right of appeal is important and should be considered in future legislation.	This is provided for under clause 180, as explained in Recommendation 11.

15	Appointment to the IPT should be limited to a term of four years, renewable once for a further four years.	The current appointment periods allow members of the IPT to develop expertise in a complex area. We will continue to keep appointments to the IPT under review.
16	The judicial commissioners should have a statutory right to refer cases to the IPT where they find a material error or arguable illegality or disproportionate conduct.	Clause 171 provides that if the Investigatory Powers Commissioner identifies an error they must consider whether it is serious. If they consider it to be a serious error, they must inform the IPT. If the IPT agrees that it is a serious error, it is for the IPT to decide whether it is in the public interest and in the interest of national security for that person to be informed.
17	The Intelligence Services Commissioner, Interception of Communications Commissioner's Office, and the Office of Surveillance Commissioners should be replaced by a new single independent organisation: a National Intelligence and Surveillance Office (NISO). This organisation should be placed on a statutory footing and its independence guaranteed by statute.	Clause 167 of the draft Bill establishes in statute the office of the Investigatory Powers Commissioner. The Investigatory Powers Commissioner will replace the role of the Intelligence Services Commissioner, the Interception of Communications Commissioner and the Chief Surveillance Commissioner. The Bill also provides for the appointment of Judicial Commissioners to support the Investigatory Powers Commissioner, and the IPC may delegate functions to the Judicial Commissioners as appropriate.
18	A NISO should have an office based outside of the Whitehall departments, have a public profile and be led by a senior public official. The new organisation should be staffed by appropriate persons with technical, legal, investigative and other relevant expertise (for instance in privacy and civil liberties). The new organisation would have four main areas of responsibility: • Inspection and audit • Intelligence oversight	The office of the Investigatory Powers Commissioner will be based outside Whitehall. Clause 176 requires the Secretary of State to provide the Investigatory Powers Commissioner with the staff, accommodation, equipment and facilities that they consider necessary for the IPC to fulfil its functions. The IPC will be provided with increased resources, including technical, legal and communications expertise so that they are effective and visible.

	• Legal advice • Public engagement.	
19	A NISO should provide support and assistance to the Investigatory Powers Tribunal and the judicial commissioners.	Clause 172 requires a Judicial Commissioner to give the IPT any assistance the IPT may require, including the Commissioner's opinion to inform the IPT's decision in a matter.
20	Urgent improvements are necessary in order to expedite the mutual legal assistance treaty (MLAT) process and, in particular, to the UK–US process in managing data requests. We support the practical reforms suggested by Sir Nigel Sheinwald to the existing MLAT between the UK and the US, to include the greater standardisation of processes, training and improved guidance. The scope for a new and wider international framework between like-minded democratic countries should also be seriously investigated with the aim of allowing law-enforcement and intelligence agencies more rapid access, under agreed restrictions, to relevant data in cases of serious crime and for urgent counter-terrorism purposes.	The UK has been working with international partners to improve the quality of MLAT requests and streamline the process for under our existing bilateral arrangement with the US. We are separately taking forward Sir Nigel Sheinwald's recommendation for a new international framework, and are exploring with partners how such an agreement might work in principle.

21 December 2015

Human Rights Watch—written evidence (IPB0123)

Introduction and Summary

1. Human Rights Watch welcomes the opportunity to provide comments on the draft UK Investigatory Powers Bill (IP Bill). Human Rights Watch is an international nongovernmental organization that monitors and reports on human rights in about 90 countries around the world. We have documented the harms of overbroad and unchecked surveillance for the work of journalists, lawyers, and civil society organizations and advocated for stronger protections for the right to privacy in the digital age in the UK, US, and globally.

2. The Internet has become central to nearly every aspect of our lives and is the cornerstone of today's modern global economy. It has also helped advance global human rights, enabling independent civil society and individuals to advocate for their rights and demand accountability from their governments. At the same time, we also now live in an age of "big data," when our communications and activities routinely leave rich digital traces that can be collected, analyzed, and stored at low cost. In parallel, commercial imperatives drive a range of companies to amass vast stores of information about our social networks, health, finances, and shopping habits.

3. These trends have led to what many have deemed the "golden age of surveillance," where law enforcement and security agencies have access to an unprecedented amount of investigatory material enabled by the digital world, including entirely new forms such as location data or web browsing histories.[414] Declining costs of computing and data storage have also removed many financial or practical constraints to conducting surveillance or data collection.

4. Unfortunately, corresponding legal protections for the right to privacy have not kept pace with technological change. The UK Government's Regulation of Investigatory Powers Act of 2000 was passed years before the advent of modern social media or widely available smart phones. New digital investigatory techniques like equipment interference/computer network exploitation (CNE) were not even contemplated by many policymakers 15 years ago.

5. Human Rights Watch believes the UK's surveillance legislation should be overhauled so that a broad range of investigatory powers are subject to the rule of law and adequate oversight and supervision, and to ensure privacy is protected. However, the draft IP Bill introduced on November 4, 2015 falls gravely short in preventing unjustified or disproportionate breaches of privacy and other rights and in providing

[414] Peter Swire, "'Going Dark' Versus a 'Golden Age for Surveillance,'" Center for Democracy & Technology, November 28, 2011, https://cdt.org/blog/%E2%80%98going-dark%E2%80%99-versus-a-%E2%80%98golden-age-for-surveillance%E2%80%99/ (accessed December 21, 2015); Peter Swire, Testimony at US Senate Judiciary Committee Hearing, "Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy," July 8, 2015, http://www.judiciary.senate.gov/imo/media/doc/07-08-15%20Swire%20Testimony.pdf (accessed December 21, 2015).

transparency, adequate oversight, or access to effective remedies. Many of the provisions are vaguely and broadly drawn, leaving the public unsure of the scope and scale of measures it enables or how privacy will be affected by those measures. In its current form, the bill would legitimize mass surveillance and extraterritorial warrants served on companies outside the UK for surveillance and device hacking, which sets a worrying precedent that could jeopardize the rights of UK citizens and that other governments, including abusive regimes, might follow.

6. Human Rights Watch urges the joint committee to incorporate the following in its recommendations to Parliament:
    a. ***Require meaningful judicial authorization:*** Independent, prior judicial authorization should be required for all powers authorized under this act and judges should be empowered to review the merits of the warrant application and make an independent determination of its legality, necessity, and proportionality.
    b. ***Bulk Data Collection and Interception are Fundamentally Disproportionate:*** Authorities should be required to demonstrate to an independent judicial authority that the measures sought are the least intrusive means for achieving the defined goal, that more tailored means have been exhausted, and that the bulk measures would be effective at achieving the defined goal. The larger and more indiscriminate the measure of collection, the more difficult this standard will be to meet, foreclosing bulk collection as a routine or standard measure.
    c. ***Refrain from Undermining Encryption and Digital Security:*** Strong encryption and analogous measures are essential to both privacy and security online. Requirements that telecommunications or Internet companies "maintain technical capabilities" are not sufficiently defined in the bill to ensure they do not disproportionately harm rights. The bill should be amended to ensure authorities are prohibited from imposing obligations on Internet service providers to weaken security measures or design their systems to incorporate measures for exceptional access into encryption by UK authorities.
    d. ***Equipment Interference Powers Require More Scrutiny:*** Equipment interference powers raise novel technical and legal issues that deserve greater scrutiny before the bill moves forward. Given the potentially broader harm to cybersecurity, Human Rights Watch questions the proportionality and necessity of equipment interference as a whole, and these concerns are more acute for bulk equipment interference. The committee should seek greater public transparency from intelligence and law enforcement agencies into how equivalent provisions have been applied under current law, and how this might change under the IP Bill. The bill should also be amended to more narrowly define the information and equipment that can be targeted under targeted equipment interference warrants.
    e. ***Extraterritorial Impact:*** The bill should be amended to forbid authorities from serving warrants on service providers outside the UK. Otherwise, the bill in its

current form could set a deeply troubling global precedent. Other governments could demand of companies similar access, potentially including requests for data of UK citizens by authoritarian governments abroad.

f. ***Remedy Remains Ineffective:*** The draft bill falls short in providing adequate transparency and removing the significant barriers to redress that exist in the current system. The bill should require notification to individuals whose communications have been intercepted or whose data has been collected, though notice could be delayed under specified circumstances. The Investigatory Powers Commissioner and other oversight bodies should be required to inform individuals when it is determined that their rights have been breached so they can seek recourse.

The Right to Privacy in the Digital Age

7. Digital technologies have enabled surveillance on an unprecedented scope and scale. A landmark 2014 report by the UN High Commissioner for Human Rights examined the regulation of surveillance powers globally and found that many governments have failed to meet their obligations to protect privacy under international human rights standards. The High Commissioner found practices in many states revealed "a lack of adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight."[415] Combined with a "disturbing lack of governmental transparency," these failings have "contributed to a lack of accountability for arbitrary or unlawful interference in the right to privacy." Accordingly, the High Commissioner provided guidance for states to ensure surveillance is conducted consistent with human rights requirements:

    a. ***Mass surveillance is by nature indiscriminate, arbitrary, and disproportionate.*** Large-scale collection practices often fall afoul of the requirement of proportionality. Proportionality requires that the government use the least intrusive means to achieve a legitimate aim and the onus is on the government to show that it has complied with that requirement.
    b. ***Communications data is often just as sensitive*** and revealing as the content of communications and merits stronger protection than many national laws currently grant. This was implicitly recognized by the Court of Justice of the European Union (CJEU) in *Digital Rights Ireland* when it invalidated the EU's Data Retention Directive, noting that the blanket nature of data retention mandates flouts the principle of proportionality.[416] The UN High

[415] UN Human Rights Council, Report of the Office of the United Nations High Commissioner for Human Rights, "The Right to Privacy in the Digital Age," U.N. Doc. A/HRC/27/37, June 30, 2014, http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc (accessed December 12, 2015).

[416] *Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, Judgement, April 8, 2014, Joined Cases C‑293/12 and C‑594/12, ECLI:EU:C:2014:238, http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=lst&docid=150642&occ=first&dir=&cid=314051 (accessed December 21, 2015); Cynthia Wong, "Dispatches: Victory for Digital Privacy on Data Retention," Human Rights Watch, April 9, 2014, https://www.hrw.org/news/2014/04/09/dispatches-victory-digital-privacy-data-retention.

Commissioner for Human Rights also noted that "Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association. The very existence of a mass surveillance programme thus creates an interference with privacy. The onus would be on the State to demonstrate that such interference is neither arbitrary nor unlawful."[417]

c. The High Commissioner found that mandatory third-party data retention requirements, where the government requires Internet or mobile service providers to store data about all customers that the government can later access, "***appear neither necessary nor proportionate***" since they interfere with the privacy of all users, regardless of whether they are under suspicion of wrongdoing.
d. States should also ensure ***effective oversight to safeguard against abuse, as well as remedy*** for violations of rights linked to digital surveillance. Prior, independent judicial authorization is best practice in this regard, along with oversight from all branches of government.

8. In July 2015, the UN Human Rights Committee reiterated many of these conclusions in its review of the UK's implementation of the Article 17 right to privacy under the International Covenant on Civil and Political Rights (ICCPR). The Committee expressed concern that the UK's laws "allows for mass interception of communications and lacks sufficient safeguards against arbitrary interference with the right to privacy" and provided weaker safeguards for interception of so-called "external communications" sent or received outside the UK. The Committee called on the UK government to do the following:[418]
    a. Ensure surveillance and data collection practices comply with the ***principles of legality, proportionality, and necessity, regardless of the nationality or location of the individuals*** whose communications are under surveillance.
    b. Ensure ***robust oversight systems over surveillance, interception, and intelligence sharing*** are in place, including by providing for "***judicial involvement in the authorization of such measures in all cases***" and strong and independent oversight mandates to prevent abuse.
    c. Ensure access to communications data is limited to the extent ***strictly necessary for prosecution of the most serious crimes*** and is dependent upon ***prior judicial authorization***.
    d. Ensure ***access to effective remedies*** to address cases of abuse.

[416] UN Human Rights Council, Report of the Office of the United Nations High Commissioner for Human Rights, "The Right to Privacy in the Digital Age," U.N. Doc. A/HRC/27/37, June 30, 2014, para 20.
[417] Ibid.
[418] UN Human Rights Committee, "Concluding observations on the seventh periodic report of the United Kingdom of Great Britain and Northern Ireland," U.N. Doc. CCPR/C/GBR/CO/7, August 17, 2015, http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G15/182/29/PDF/G1518229.pdf?OpenElement (accessed December 21, 2015).

9. The current draft of the Investigatory Powers Bill falls fatally short of these requirements and should be revised considerably. We highlight several issues of particular concern below and urge the Joint Committee to raise these concerns in its report on the bill and directly with the government.

Require Meaningful Judicial Authorization

10. In introducing the IP Bill on November 4, 2015, Home Secretary Theresa May stated it would create a "world-leading oversight regime," requiring a "double-lock" of executive and judicial approval.[419] However, while the bill is an improvement over the current framework, the bill's authorization mechanisms do not hold up under scrutiny and are inadequate to safeguard against arbitrary and unlawful intrusions on privacy.

11. The bill provides only a limited role for judicial commissioners in approving warrants for various investigatory powers throughout the bill, applying "the same principles as would be applied by a court on an application for judicial review." Thus, the judges would only be able to assess whether the authorities followed the correct procedure and acted reasonably and within their powers. The bill does not contemplate independent, substantive judicial review of executive decisions, nor of the evidence presented by authorities that supports them. In all, this structure is inadequate to ensure effective supervision of the government's broad surveillance powers.

12. Some intrusive and potentially broad surveillance powers would not require approval by judicial commissioners. Specifically, under the bill, there is no judicial role in approving "targeted" requests to access communications data and warrants issued to companies to retain data. Given the growing recognition of the sensitivity of communications data, this omission is troubling. Similarly, judges play no role in approving broadly defined national security or technical capability notices served on telecommunications operators.[420] These notices are ill-defined and enable exceptionally broad powers. National security notices can require service providers to "carry out any conduct … for the purpose of facilitating anything done by an intelligence service under any enactment other than this Act," if in the interest of national security. Technical capability notices can impose obligations on service providers to "provide facilities or services" or "the removal of electronic protection" to any communications or data. These broadly and ill-defined powers raise novel legal and technical questions that should be subject to substantive as well as procedural prior review by an independent judge, along with scrutiny by other oversight bodies.

[419] Theresa May, Oral statement to Parliament, "Home Secretary: Publication of draft Investigatory Powers Bill," November 4, 2015, https://www.gov.uk/government/speeches/home-secretary-publication-of-draft-investigatory-powers-bill (accessed December 21, 2015).
[420] IP Bill, Clauses 188, 189

13. Authorities would also be able to proceed without even this pro forma judicial approval temporarily if they deem it "urgent," though they would need to seek approval after the fact. Whether a case is "urgent" would be decided by the person who issued the warrant, and such cases would not be limited to situations involving imminent threats to life or property. "Urgency" should be conservatively defined in the law, and the government denied the use of such collected data, as well as the use of evidence derived from such data, if on subsequent review a court determines that the initial determination of urgency was an abuse of executive discretion.

14. ***Recommendations***:
    a. Judicial commissioners should be empowered to review evidence presented in support of a warrant and make an independent determination of the warrant's legality, necessity, and proportionality.
    b. Independent judicial authorization should be required for all powers authorized under the act, including targeted access to communications data, data retention warrants, and national security and technical capability notices.
    c. Judges should have access to external technical expertise, with security clearance if necessary, in assessing the necessity and proportionality of proposed powers and warrants.

Bulk Data Collection and Interception Fundamentally Disproportionate

15. The bill provides an explicit legal basis for interception and communications data collection (including that of UK citizens) in bulk, putting longstanding practices on clear legal footing.[421] While bringing current practices within the rule of law is desirable, mass or large-scale surveillance is fundamentally arbitrary and disproportionate.

16. The right to privacy is implicated when personal data or communications are collected—in the most commonly understood use of the word—and can be violated if such collection is arbitrary, unlawful, or indiscriminate. This is true regardless of whether the information is subsequently processed, examined, or used by the government.

17. Dragnet searches or collection on large groups without some threshold showing of necessity and proportionality should be presumptively impermissible. In the US, one bulk communications data program was halted after two independent oversight bodies with access to classified information found that the program was not essential

[421] The term "bulk" is not sufficiently defined in the draft bill or existing legal frameworks. For purposes of this submission, we assume that this term could apply to a range of large-scale interception or data collection programs, including mass interception of all Internet traffic flowing through trans-Atlantic fiber optic cables, potentially nationwide collection of communications data, or other large scale programs that do not premise collection on the prior identification of a specific individual or group.

to preventing terrorist attacks.[422] This program violated the privacy of potentially millions of individuals, while providing no unique intelligence value. It would have continued to do so had the program not come to light and been subjected to independent scrutiny.

18. ***Recommendation***:
    a. Authorities should be required to demonstrate to an independent judicial authority that the measures sought are the least intrusive means for achieving the defined goal, that more tailored means have been exhausted, and that the bulk measures would be effective at achieving the defined goal. The larger and more indiscriminate the measure of collection, the more difficult this standard will be to meet, foreclosing bulk collection as a routine or standard measure.

Refrain from Undermining Encryption and Security

19. The Home Secretary has stated that the bill "will not ban encryption or do anything to undermine the security of people's data."[423] However, in addition to imposing general duties to give effect to warrants, the bill would allow authorities to require private telecommunications or Internet companies to "maintain technical capabilities" to assist with the execution of warrants. The bill gives as one example the "removal of electronic protections" used by the company to safeguard communications or data.[424] Depending on how these provisions are applied, they could be used to undermine the security of popular Internet services, especially if they require companies to weaken encryption or redesign encrypted services to enable "back doors" or exceptional access for UK authorities.

20. Strong encryption and analogous measures designed to secure data are essential to safeguarding privacy and other rights online.[425] It is also the cornerstone of security in the digital age, shielding ordinary users from cybercrime, identify thieves, and other malicious actors. As a group of prominent computer scientists and security experts have stated, the modern world is "completely reliant on secure communications for every aspect of daily lives, from nations' critical infrastructure, to personal privacy in daily life, to all matters of business. … It is impossible to operate the commercial Internet or other widely deployed global communications network with even modest security without the use of encryption."[426] Intentionally

[422] Peter Swire, "The USA FREEDOM Act, the President's Review Group and the Biggest Intelligence Reform in 40 Years," Privacy Perspectives Blog, June 8, 2015, https://iapp.org/news/a/the-usa-freedom-act-the-presidents-review-group-and-the-biggest-intelligence-reform-in-40-years (accessed December 21, 2015).
[423] Theresa May, Oral statement to Parliament, "Home Secretary: Publication of draft Investigatory Powers Bill," November 4, 2015.
[424] IP Bill Part 9, clause 189.
[425] UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, U.N. Doc. A/HRC/29/32, May 22, 2015, http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx (accessed December 21, 2015).
[426] Harold Abelson, et al., "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications," Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory Technical Report, July 6, 2015, http://dspace.mit.edu/handle/1721.1/97690 (accessed December 21, 2015).

compromising encryption, even for arguably legitimate purposes, weakens everyone's security online, not just those suspected of wrongdoing, and can put even government systems at risk.

21. Any provisions that could be interpreted to require companies to weaken secured services or build back doors into encryption raises serious human rights concerns. A requirement of either decryption or assured decryptability for all online communications, including the billions that involve no suspicion of threat to public order or national security, could not be proportionate and has never been shown to be necessary.

22. ***Recommendations***:
    a. The bill should be amended to ensure authorities are prohibited from imposing obligations on Internet service providers to weaken security measures or design their systems to incorporate measures for exceptional access into encryption by UK authorities.
    b. The committee should seek greater public transparency from intelligence and law enforcement agencies into how equivalent provisions have been applied under current law, and how this might change under the IP Bill.

Equipment Interference Powers Require More Scrutiny

23. The draft bill provides an explicit legal basis for equipment interference/computer network exploitation (that is, hacking), placing existing practice on firm legal footing for the first time. Hacking allows law enforcement to surreptitiously access data and communications directly from personal devices and other equipment, which can allow authorities to bypass encryption. The draft bill contemplates both targeted and bulk equipment interference, and warrants must be approved by judicial commissioners. These provisions allow authorities to compromise a broad range of equipment, beyond personal devices used by individuals suspected of a crime, and could include equipment belonging to major Internet companies. Warrants may also authorize a wide range of conduct to acquire broadly defined categories of information.

24. These capabilities raise novel technical and legal issues that deserve greater scrutiny before the bill moves forward. Hacking is a fundamentally more intrusive form of surveillance than interception or data collection. A single laptop or mobile phone routinely contains the equivalent of our personal filing cabinets, photo albums, years of correspondence, address books, banking information, shopping history, dating history, medical records, and bookshelf in one device. Hacking into a device can allow access to this data, along with the capture of passwords and real-time video or audio monitoring through the device's microphone and built-in camera. Once a device has been hacked, authorities can covertly delete or alter files and systems, or even sabotage or destroy them.

25. In addition, hacking can also cause broad and unintentional harm to devices and networks, affecting a broad range of users who are not suspects or intelligence targets. Many techniques used to compromise equipment involve identifying vulnerabilities in widely used software (e.g., Microsoft Word, Android) or hardware, and exploiting those vulnerabilities to install malware onto the device. If governments are permitted to hack into devices, they have no incentive to disclose vulnerabilities to the private sector so they can be fixed. These same vulnerabilities are also used by cybercriminals and other malicious actors to steal personal data for profit, so leaving them unfixed weakens security for all users.

26. Given these broader harms, we question the proportionality and necessity of equipment interference as a whole, and these concerns are even more acute for bulk equipment interference powers. The committee must elicit and publicize more evidence detailing how these powers are currently being used. Otherwise, it is difficult to assess the legitimacy of these measures.

27. ***Recommendations***:
    a. The committee should seek greater public transparency from intelligence and law enforcement agencies into how they are using equipment interference powers under current law, and how that might change under the IP Bill.
    b. The bill should be amended to more narrowly define the information and equipment that can be targeted under targeted equipment interference warrants.
    c. Bulk equipment interference powers should be removed from the bill.

Extraterritorial Impact

28. The draft bill allows certain warrants to be served extraterritorially on communications service providers located outside the UK, who must take "reasonably practicable" steps to comply. When deciding whether it is reasonably practicable to take certain steps, UK authorities will take into account whether the warrant might require the service provider to violate the laws of another jurisdiction.

29. Mutual legal assistance arrangements are used by governments, including the UK, to obtain communications or data held in other jurisdictions for the investigation or prosecution of criminal offences. To obtain access to content held by US Internet companies, for example, UK authorities generally must make requests to US authorities under an existing mutual legal assistance treaty (MLAT) since US companies are prohibited from disclosing content without a warrant meeting US standards.[427] However, the IP Bill allows UK authorities to circumvent existing mutual legal assistance arrangements that govern cross-border law enforcement requests for content by permitting them to serve warrants directly on companies outside the UK. This could set a deeply troubling global precedent and undermine the rule of law.

[427] See Jennifer Daskal and Andrew K. Woods, "A New US-UK Data Sharing Treaty?" *Just Security*, June 23, 2015, https://www.justsecurity.org/24145/u-s-u-k-data-sharing-treaty/ (accessed December 21, 2015).

It also raises issues of transparency and legal certainty in cases where such warrants present direct conflicts between the laws of the UK and other countries, as it would when seeking content of communications from US service providers.

30. At heart, the UK would be asserting jurisdiction over data held in any country by any company that provides services in the UK. This would set a dangerous precedent, one that would spark a race to the bottom for privacy as other governments would demand of companies similar access, potentially including requests for data of UK citizens by abusive governments abroad.

31. ***Recommendations***:
    a. Remove clauses that allow authorities to serve warrants on communications service providers outside the UK.
    b. Work with the US and other governments to enhance existing Mutual Legal Assistance arrangements for cross-border law enforcement requests and improve their speed and efficiency, consistent with human rights requirements.

Remedy Remains Ineffective

32. The bill would provide for a new right to appeal decisions by the secretive Investigatory Powers Tribunal (IPT) before the Court of Appeal. However, it would fall short on providing the transparency so lacking in the current system.

33. The IPT, located under the Home Office, is the sole judicial body where individuals and organizations who suspect they have been under "unlawful" surveillance can file a complaint. Complainants have no access to the government's evidence nor ability to question it. They also have no access to the tribunal's deliberations nor the tribunal's rationale where complaints are rejected. Compounding these transparency issues, the bill would allow the Court of Appeal to hear appeals from the IPT wholly or partly in "closed material proceedings," which would exclude applicants and their lawyers from the hearings.

34. The bill also would not remove barriers to redress in the current system since users are never notified that they have been under surveillance, and so generally do not know to seek review at the IPT. While the newly created investigatory powers commissioner would be required to inform individuals of "serious errors" that affect them, the mere fact that an individual's fundamental rights have been breached would not be sufficient by itself to be considered "serious" under the bill. In addition, before notice can be given, the Investigatory Powers Tribunal must agree that the error is serious and that it is in the public interest to notify affected persons. More information is needed about how these terms will be applied in practice.

35. ***Recommendations***:

a. Require notification to individuals whose communications have been intercepted or whose data is collected to enable them to seek review and redress. Notice could be delayed until after an investigation has been closed (or longer in certain circumstances) where immediate notice would seriously jeopardize an ongoing investigation or there is an imminent risk of danger to human life. Requests to delay notification should be reviewed and authorized by independent judges.
b. Hearings at the IPT should be open and public, unless the tribunal determines closed proceedings are necessary for national security or other legitimate purposes. Security-qualified lawyers, and where appropriate other lawyers and applicants, should be allowed to attend hearings, hear arguments, and review evidence before the court.
c. The Investigatory Powers Commissioner and other oversight bodies should be required to inform individuals when it is determined that their rights have been breached so they can seek recourse.

Conclusion

36. Thank you for the opportunity to submit written evidence on the draft IP Bill. If we may be of any additional assistance, please do not hesitate to contact us.

21 December 2015

Dr Julian Huppert—written evidence (IPB0130)

Introduction

1. Thank you for the invitation to provide written evidence to this important Joint Committee on the Investigatory Powers Bill (IPB).[428] This is an important and fundamental piece of legislation, that is unlikely to be substantially revisited for decades, and it is very important that it receives full and detailed pre-legislative scrutiny. It is a shame that the Committee has been given a relatively short timetable to do the very substantial amount of work to fully understand this technically and legally complex piece of legislation.

2. I served on the Joint Committee on the Draft Communications Data Bill (CDB), the predecessor to the IPB. We had five months to scrutinise a relatively simpler piece of legislation, including four months to take oral evidence. Even then, there was a lot of work involved, and our understanding both as individuals and a committee increased right through to the end, especially given that the Home Office did not provide some key information we could use in our report until the last moments. I do not envy the task this Committee has in front of it.

3. **As you are aware, our committee was unanimous in its strong criticism of the draft CDB saying among other things that various aspects of the evidence provided by the Home Office were 'misleading'.[429]**

4. We concluded that the CDB 'pays insufficient attention to the duty to respect the right to privacy, and goes much further than it need or should for the purpose of providing necessary and justifiable official access to communications data'.[430] Partly as a result of that unanimous conclusion, the Bill was never presented to Parliament.

5. It is important to highlight that our criticism and concern predated any of the Snowden revelations, which showed just how much bulk data collection was being conducted without the benefit of clear and transparent legal authorisation under RIPA or other legislation. As the former Chair of the CDB Committee, Lord Blencathra, also a former Conservative Home Office Minister, said, 'Some people were very economical with the actuality. I think we would have regarded this as highly, highly relevant. I personally am annoyed we were not given this information'. I am confident that our criticisms of the CDB and the veracity and completeness of the evidence provided to us by the Home Office would have been stronger had we known of those revelations in time.

6. The Snowden revelations are a large part of the reason that this legislation exists in the form it does, covering such a wide range of previously unavowed powers. It is absolutely right to codify such substantial, wide-scale and potentially highly intrusive

[428] Some of the information in this submission has been provided to the Science and Technology Select Committee in their inquiry into the same Bill.
[429] Report on the draft CDB, summary and paragraphs 36, 39, 267, 269 and 323
[430] Ibid. Summary

powers such as these. As Sir David Omand, former Director of GCHQ and former Permanent Secretary at the Home Office, wrote in #intelligence, '**Democratic legitimacy demands that where new methods of intelligence gathering and use are to be introduced, they should be on a firm legal basis and rest on parliamentary and public understanding of what is involved'**. I agree entirely with him, and welcome the relative transparency in this draft bill, especially in comparison with the previous regime, which relied on internal interpretation of very broad statutes. Parliament should decide.

7. However, just because a power has been previously asserted to exist by the Agencies, and has been implemented, is not in and of itself a reason why Parliament should be required to continue it in this legislation. Parliament, initially acting through this Committee can and should insist on clear evidence from the Home Office as to why each and every power is needed, why it is both necessary and proportionate for each power to be allowed, and to show that the disbenefits, including privacy violations, are clearly lower than the benefits. The onus should be on the Home Office to prove this in each case, not merely to assert utility. This has not been done as of the time of writing for any of the powers requested.

8. Simply giving case studies where a particular power could be useful to the Police or Agencies is far from satisfactory. Almost any power could be justified under that argument, even if any reasonable person would consider it excessive. To take one extreme example (one that to the best of my knowledge is not being advocated by anyone), there is no doubt at all that if there were a new legal requirement for everyone in the UK to have a surgically implanted GPS tracker, this could be useful to the Police or Agencies. Crimes could be detected, terrorist acts potentially averted, lives saved – but no one would really consider it to be a reasonable response to the undoubted challenges we all face. It would not be practicable, would not be proportionate, would not be necessary, and the harms caused would massively exceed the benefits. **The Committee should require the Home Office to systematically provide detailed evidence for each power requested, so that the Committee can rationally determine whether each power is necessary in the legislation.**

9. It is particularly important in this context to consider **the resources needed to wade through very large data sets.** In almost every terrorist case, it later transpires that **there was information already known to the Agencies about the culprits**. However, resource constraints meant that appropriate action was not taken. Greater resource for the Agencies is likely to be more beneficial than wide-ranging extra powers.

10. One clear example of this was with the murder of Fusilier Lee Rigby. One of the murderers, Adebowale, was of sufficient interest to MI5 that they submitted an application to the Home Secretary for 'further intrusive techniques'. As a result of 'staffing pressures' in MI5, this application was not submitted promptly to the Home Office, which only received the application the day before the attack. The Intelligence and Security Committee wrote that 'It therefore seems likely that – had the seven day target for submission been met – these further techniques would have been in

place during the week before, and on the day of, the attack'.[431] Had this been processed promptly, it is surely reasonable to think that the intrusive measures taken could have detected and prevented the attack. It is also noteworthy that the other murderer, Adebolajo, 'was under intensive surveillance for a significant period of time', with MI5 stating that 'from an investigative perspective, we threw the kitchen sink at it'.[432]

11. Another clear example involves the failure of UK policing to tackle paedophiles discovered from Project Spade. In essence, Canadian Police closed a child abuse ring, freeing hundreds of children from exploitation, and seizing customer records. CEOP were given details of 2,345 people who had been customers for this material. However, they failed to act on this information for 14 months, citing lack of resources. Among the people who could have been investigated was Dr Myles Bradbury, a paediatric oncologist at Addenbrooke's Hospital, Cambridge, who has now been convicted of abusing children in his care. He could and should have been stopped sooner, and no new powers were required. **Resources should be focused on making the most of existing powers before any requests are made for additional powers.**

12. The hunt for useful information among intelligence traffic has often been described as hunting for a needle in a haystack. **It seems clear that the best way to do this is by providing the resources to use a magnet, rather than collecting more hay to add to the pile.**

13. In this evidence I seek to cover the whole range of the Bill. In some areas, I have had to leave out details in the interests of length, and I have focused on the broad principles of each section.

14. The Committee will also be aware that I am organising, on behalf of the Foundation for Information Policy Research and the Policy Institute at King's, a conference on the 7th January to discuss the Bill. All members of the Committee have been invited to attend any or all of the sessions, as have the clerks and advisors. We hope to make the video of this available as well, and I hope the Committee will be able to take into account what is said there by a very broad range of experts.

Lawful Intercept – part 2

15. Powers for lawful intercept currently exist explicitly in RIPA, and are relatively clearer than many other areas of RIPA. It is clearly right that such powers should exist in some form, as long as it is highly targeted. However, there are still important issues about how these powers are authorised and operated.

16. The UK is currently unusual in having Ministerial authorisation of interception requests – indeed, we are the only Five Eye nation not to use judges in the

[431] Intelligence and Security Committee of Parliament Report on the intelligence relating to the murder of Fusilier Lee Rigby, p. 108, para. 332
[432] Ibid., p. 42, para 108.

authorisation process. David Anderson QC, the Independent Reviewer of Terrorism Legislation, proposed that we should create a system of judicial authorisation for all warrants.[433] However, the current legislation does not do this. Instead, it creates a process of judicial review of Ministerial decisions, which is a far weaker and more complex approach. In particular, Judicial Commissioners, appointed personally by the Prime Minister with no parliamentary or other approval (clause 167), are only assessing whether the Ministerial decision was unreasonable, rather then assessing the case afresh. This severely limits their utility. It is also notable that even if a Prime Ministerially appointed Judicial Commissioner holds that the Minister was unreasonable, there is an appeal for the government to the Prime Ministerially appointed Investigatory Powers Commissioner.

17. David Anderson QC has strongly made the case for judicial authorisation, rather than judicial review. He emphasises the benefits of liberating time for the Home Secretary – who last year apparently personally authorised 2,345 warrants. He further highlights the benefits in public confidence and of increasing access to information from US providers (where judicial authorisation is the norm).

18. **The Committee should strongly consider recommending the Government follow the recommendations of David Anderson QC and many other governments, and implement a full system of judicial authorisation as he outlines.**

19. RIPA authorises interception warrants very clearly only for one person or a single set of premises,[434] and requires the Secretary of State to sign the warrant personally, except in urgent cases, where the Secretary of State must have expressly authorised the issue of the warrant.[435] There is no provision in law for warrants to apply to multiple people. However, in practice, so-called thematic warrants have been used across multiple people of premises. While there may well be good practical arguments for this, as a matter of principle the wording of the statute should be followed rather than being ignored.

20. The IPB specifies in clause 13 that warrants may apply to multiple people and multiple premises. This makes the power explicit, in a way that it was not previously, but there are minimal safeguards in place. In particular, clause 26(2)(a) allows, for the first time, for names or premises to be added to a warrant by a senior official, with no express authorisation from a Minister, and no involvement of a Judicial Commissioner. **This change would represent the first time that interception was allowed without any ministerial or judicial authorisation. The Committee should recommend that the same level of ministerial and judicial authorisation is required to add an individual to an existing warrant as to create a new warrant.** Otherwise, it is entirely possible to foresee a situation where a Minister and Judicial Commissioner authorise a warrant with particular limits on people or premises, only to see the limits changed afterwards without their approval. It is notable that the protection for MPs etc. is applied to these changes, although other protections are not.

[433] A Question of Trust, section 14.47-14.57
[434] RIPA 2000, s8(1)
[435] RIPA 2000, s7(2)

21. Section 94 of the Telecommunications Act is an incredibly broad powered piece of legislation, that authorises a Secretary of State to direct a telecommunications operator to do anything at all necessary 'in the interests of national security or relations with the government of a country or territory outside the United Kingdom'. The only safeguard in the legislation is a requirement that any use be reported to Parliament – unless disclosure would be 'against the interests of national security or relations with the government of a country or territory outside the United Kingdom, or the commercial interests of some other person'. As a result of this exemption, use of the power has never been reported to Parliament. It was not examined by the ISC or any of the Commissioners until this year. The Interception of Communications Commissioner reported in 2015 on the use of this legislation, saying;

> "*There are, however, some considerable challenges in this regard. The challenges stem from the fact that the directions are secret as allowed for by statute, can be given by any Secretary of State and do not automatically expire after a certain period. There does not appear to be a comprehensive central record of the directions that have been issued by the various Secretaries of State. My office is therefore not yet in a position to be able to say confidently that we have been notified of all directions."*[436]

22. It has now been avowed that it was used by GCHQ to collect bulk phone records without explicit approval or awareness from Parliament, and in contravention of the principles in RIPA.

23. **It is very welcome that this secretive and broad-spectrum legislation is to be repealed**, but it is concerning that some elements of it have been re-introduced in the IPB. Clause 39 allows any interception if requested by another country. None of the protections otherwise applied to interception apply to this clause, which empowers interception of UK nationals for other countries with even fewer safeguards than apply to the UK Agencies. **The committee should recommend that this power be subject to the same constraints and oversight as other interception powers.**

24. Clause 188 is even broader, allowing anything at all to be done by notice of the Secretary of State to a telecommunications provider. Although there is provision for review of such a notice by the Secretary of State in consultation with the Technical Advisory Board and the Investigatory Powers Commissioner, unlike other powers, there is no judicial approval or authorisation, and no safeguards for Parliamentarians, journalists or others. Indeed, the Secretary of State can confirm a challenged notice even if the Investigatory Powers Commissioner asserts on the evidence that the notice were disproportionate. **This proposal should be changed, to restore the safeguards presented in the rest of the bill in terms of judicial authorisation and oversight, as well as other protections and safguards.** Otherwise, there is a very real

[436] Half-yearly report of the Interception of Communications Commissioner - July 2015, p. 13 para 4.4.

risk that powers will be implemented using this unprotected power rather than the rest of the legislation.

Part 3 – Communications Data

25. This section largely reproduces existing powers to access communications data. There is clearly a benefit from accessing such information where it is held (I comment in Part 4 about the merits or otherwise of holding so much data and specific types of data).

26. Authorisation for Communications Data access is in almost all cases neither judicial not ministerial, but is processed internally by the organisations applying for the data. The exception is local government, where there is a requirement for judicial authorisation of communications data requests. This could be extended to other requests, particularly for more intrusive communications data requests. The vast majority of such requests are 'reverse directory lookups', which would not require judicial approval. **The Committee should consider recommending that the judicial approval system for local government be extended to other bodies for more intrusive data requests.**

27. Clause 47 requires sensibly that internal authorisation may not be performed by an officer involved with the investigation being carried out. There is however an exemption for small public authorities, where they may not have enough staff to have someone independent. Rather than exempting such authorities, **they should be required to either collaborate to provide an independent body which can authorise the request, or have judicial authorisation.**

28. The request filter described in clauses 51 *et seq.* are described as privacy enhancing. However, they in fact allow for very substantial broadening of the ability of public authorities to engage in fishing expeditions for individuals. **The committee should ask for further safeguards on the use of the request filter to ensure that it is not able to be used on an over-broad scale.**

29. Clause 61 requires judicial authorisation where the *purpose* of a request is to identify a journalistic source**. This should be broadened to any case where the request is likely to or may reveal a journalistic source**. In addition, it should be spelt out in law that the **Judicial Commissioner should have regard to the benefits of a free press** and a free society of having whistleblowers and other reasons why in general a journalistic source should be protected.

30. There is no protection equivalent to this journalists' clause for other groups who should be protected, such as doctors and lawyers. Judicial authorisation should be required for cases where the request could have impacts on legal privilege or medical confidentiality.

Part 4 – Retention of Communications Data

31. Since the Data Retention Directive, the UK Government has required retention of communications data for 12 months. The evidence base for a 12 month retention period is thin, despite the fact that it results in the keeping of substantial amounts of data on everyone in the UK. While it is true that some requests for data are made towards the end of the retention period, that is likely to be at least in part because data requests are not made promptly. **The Committee should consider recommending a reduction in the 12 month retention period, possibly associated with data preservation orders where there is suspicion that particular data may be needed later.**

32. Clause 2(b) is very broad, allowing the retention of 'all data or any description of data'. **This should be more constrained, specifying more clearly what data retention is being authorised.**

33. Previously, data retention was allowed, but there was no power for data generation – only data generated for business purposes could be required to be retained. The IPB extends this proposal to data generation, requiring for the first time data to be stored that was previously never available. In particular, it authorises the generation of Internet Connection Records.[437]

34. These, under the previous description of 'Web Logs' were discussed by the CDB Committee, who did not agree that there was a clear case made for their retention, in contrast to the importance of IP address matching. Indeed, Parliament specifically excluded web log retention in the Counter Terror and Security Act 2015 s21(3)(b).

35. Our Joint Committee reported that of our police witnesses 'neither of them provided examples that proved the importance of web logs or referred to cases that had been hampered by the current lack of web log data'.[438] David Anderson QC, the Independent Reviewer of Terrorism Legislation had a similar experience, writing that 'it was not submitted to me … that "access to weblogs is essential for a wide range of investigations'.[439] He said that there would be a requirement for a 'detailed operational case' before web log retention could be considered, and noted that many other jurisdictions excluded web log retention.

36. The Home Office has supplied what it calls an operational case for ICR retention. This is strikingly short on detail and evidence for the benefits from ICR retention, and the case is apparently based purely on 862 referrals of cases of suspected paedophiles that cannot be resolved further without ICRs. However, it is far from clear that even with ICR retention these cases could or would be progressed; there is no evidence provided to suggest that would be the case. Indeed, the document notes that there were 4215 cases in nine months where existing law would allow identification.

[437] I discuss these further in my submission to the Science and Technology Select Committee.
[438] Ibid., paragraph 78
[439] A Question of Trust, section 9.61

Strangely, however, it does not highlight how many of those cases actually were progressed, given the existing pressures on police time.

37. It is clear that ICR retention has the potential to be highly intrusive. Our report agreed that 'Web logs are at the more intrusive end of the communications data spectrum'.[440] Even though the exact webpage isn't recorded, it would be fairly clear why someone were going to websites such as www.depressionalliance.org. Even though there are constraints on the purposes for which ICR data can be obtained, **storing the data poses a serious risk that it could be released or accessed inadvertently**, as has been seen on so many occasions, such as the recent TalkTalk data breach.

38. One proposal looked at by the Joint Committee was to only retain weblog information that would identify sites used for communications.[441] This would allow the police or security services to know, for example, that someone had used Gmail, and so would enable the services to contact Google to inquire further, but without the huge collateral intrusion of keeping the entire weblog history. **This should be investigated further as a possible approach. Alternatively, the Committee should consider recommending the exclusion of ICRs from the IPB, in the absence of a proper evidence-driven operational case.**

Part 5 – Equipment Interference

39. It is right that powers for equipment interference are detailed on the face of the bill, rather than being inferred from unclear legislation, as has been the case until recently. These are powers that van be very useful when highly targeted, but pose extensive problems when used more broadly. **They are at least as intrusive as interception of communications – indeed rather more so.** Not only can they contain information about communications, they can also contain extremely private information. For example, remotely activating a webcam allows detailed monitoring of behaviour that would normally be rightly considered private. The OPTIC NERVE program collected data on a wide range of individual's webcams, with an image every 5 minutes – including a large selection of intimate or pornographic images (apparently, some 7% of all the images).

40. It is also the case that techniques developed and used to interfere with equipment run the **risk of being used by hostile or criminal organisations.** Depending on the technological approach taken, authorised interference may make it easier for unauthorised interference or monitoring to take place. **There is also the risk that the interference that is performed has unintended consequences for safety or other functioning of equipment that is interfered with.** Although this is unlikely to happen for standard pieces of equipment, where testing may be done more thoroughly, it is a very real risk when attempting to interfere with unusual equipment.

[440] Report on the draft CDB paragraph 81
[441] Ibid., paragraph 88

41. Given that equipment interference is at least as intrusive as interception of communications, it follows that it should be safeguarded at least as well. Many of the proposals in the IPB for this do echo those for interception, and **I would suggest that the committee make the same recommendations here as I suggested for interception.**

Part 6 – Bulk warrants

42. The draft IPB contains for the first time clearly laid out powers for bulk data collection in Parts 6 and 7. As Sir David Omand, former Director of GCHQ and former Permanent Secretary at the Home Office, wrote in #intelligence, '**Democratic legitimacy demands that where new methods of intelligence gathering and use are to be introduced, they should be on a firm legal basis and rest on parliamentary and public understanding of what is involved'**. I agree entirely with him, and welcome the relative transparency in this draft bill, especially in comparison with the previous regime, which relied on internal interpretation of very broad statutes.

43. However, while expressly writing the powers down in legislation is better than asserting them without clear legal source, it does not necessarily mean that the powers should be given. Equally, the fact that the Agencies have operated these powers for many years does not mean that Parliament or this Committee should feel compelled to agree that they are needed. **Most developed countries around the world do not provide such broad powers to their police or security agencies.**

44. The Committee should require the Agencies to provide clear evidence of why these powers are needed, including full cost benefit analyses, rather than simply accepting their need. The legal basis for asserting such broad powers, which are explicitly not based on suspicion, is coming under increase pressure, and the Committee may wish to explore what the alternatives would be if they were ruled illegal, and how such alternatives would compare.

45. I make the same comments about the importance of judicial authorisation rather than judicial review as I have made earlier. These apply particularly strongly to these very broad powers. Similarly, the comments made about equipment interference apply, even more strongly, to bulk equipment interference powers.

Part 7 – Bulk Personal Datasets (BPDs)

46. BPDs are a new class of data to be harvested by the Agencies. The example given for a BPD in the explanatory notes is the electoral roll, and it is hard to come up with a good reason to exclude the intelligence services from being able to access a dataset that is routinely made available to every political party.

47. However, the draft legislation does not tightly define what data sets would be covered in this legislation. Large data sets can be extremely intrusive. There is

nothing currently drafted into the IPB to constrain which data sets could be obtained and retained, even though these data sets explicitly include information pertaining to people who are not under suspicion or of interest in any way. This could include detailed vehicle mapping data, pervasive phone geolocation information, private medical information or much more. **The Committee should consider recommending significant constraints on this power, to better distinguish the data sets that are relatively less intrusive from those that are very strongly intrusive.**

Part 8 – Oversight

48. The UK has had a very fragmented oversight system, with multiple commissioners investigating some areas, while other areas (such as s94 of the Telecommunications Act 1984) not being covered by any oversight procedure. **I therefore welcome the proposal to bring all the Commissioners into one organisation.** This should help to ensure that there are no areas of activity that escape attention.

49. However, it is essential to ensure that the new organisation is well funded and given the necessary independence to ensure that it is capable of appropriately monitoring and overseeing this wide range of activities. **The Committee may wish to emphasise the need for substantial resourcing.**

50. All the Judicial Commissioners will be, as the name suggests, judges. However, many areas of oversight would benefit from other skill sets. The current Independent Reviewer of Terrorism Legislation is not a judge (instead, an eminent QC in private practice), and his role has been important in this area as well as many others. The Counter Terrorism and Security Act 2015 included a power to establish a Privacy and Civil Liberties Oversight Board, to support him in his work.

51. The Home Secretary wrote about this Board:

> *'This Board will support the role of the Independent Reviewer of Terrorism Legislation, by providing him with extra capability to carry out his role. It will offer a breadth of experience and be able to provide assistance, advice and undertake particular duties on behalf of the Independent Reviewer to support him in reviewing UK counter-terrorism legislation. It will further assist him in delivering a number of core objectives which include providing evidence to Parliamentary committees, and carrying out particular inquiries into the impact of certain issues or legislation relating to the prevention of terrorism.'*[442]

52. The Home Secretary was right to emphasise the importance of this Board, and particularly the wide range of experience needed on it, and it is therefore unfortunate that the powers have not been commenced, and the Board has not yet

[442] Home Office Consultation on establishing a UK Privacy and Civil Liberties Board, December 2014, p. 3

come into existence. **The Committee may wish to recommend that the necessary regulations be laid to enable the Board to be formed.**

53. There are a number of examples where people are wrongly target for surveillance, whether because of faulty intelligence, or technical error. According to the Interception of Communications Commissioner, in 2014 998 errors were reported to his office. The vast majority of these resulted from errors by the public authorities requesting the data.[443]

54. These errors can have serious consequences. As identified by the Commissioner, this has led to a number of cases where police visited premises unconnected with the investigation, and other cases where personal data was incorrectly disclosed. This can cause clear harm to the people affected. **There should be a clear provision for notification for people who have been subject to surveillance in error, and appropriate compensation. The Committee should also consider calling for a more general notification system for those subjected to surveillance, after it is safe and practical to do so.**

Part 9 – National Security Notices and Encryption

55. One highly controversial element leading up to the publication of the IPB was around the status of encrypted messages. The Prime Minister has argued that we should not "allow a means of communication between people … that we cannot break". He has since clarified that his intention was not to ban encryption, but to ensure that it would be possible in principle to decrypt any message.

56. While this seems on the face of it a reasonable proposition, it is technically unachievable. Relatively simple public/private key encryption systems such as Pretty Good Privacy have been around for many decades, and are relatively easy to implement. However, they are very hard to break, and the source code is publicly and widely available. It is worth noting that in 1993 the US government investigated Phil Zimmerman, the creator of PGP, for 'munitions export without a license'. This case was dropped several years later.

57. There is no central repository for the decryption keys for PGP, and so there is no way that any central organisation can decrypt the messages without exhaustive computational effort. PGP can easily be made exponentially harder to break by using longer keys, and even if that were to be breakable, such as in theory by the advent of quantum computing, there are other unbreakable encryption methods.

58. For example, a one-time pad is provably unbreakable, if it is used properly. Quantum key distribution allows effectively for secure creation of shared one-time pads, and is already available commercially in some instances. **Someone who is sufficiently**

[443] Half-yearly report of the Interception of Communications Commissioner - July 2015, p. 16

determined to communicate in an encrypted fashion will be able to do so unbreakably.

59. Many people will, however, use readily available security methods rather than implementing higher levels of security, and so it might be possible to require backdoors into communications, effectively allowing a master key that would decrypt messages when required. This could be built into commercial communications tools.

60. However, there is a high price to pay for engineering insecurity into a once secure system. It is impossible to guarantee that a backdoor could not be accessed by another organisation, whether a criminal gang, or a foreign power. A master key can be stolen. **The only way to ensure that there is no such vulnerability is not to have a back door in the first place.**

61. This is particular evident when considering tools such as TOR. Tor was designed explicitly to enable dissidents in authoritarian regimes such as China and North Korea to be able to communicate securely and bypass state monitoring, and was part funded by the US government for that purpose. It can also be used to bypass any other state's monitoring for exactly the reasons that make it safe to use in China and North Korea. **It is not technically possible to produce a tool that is completely secure in some countries but open in others.**

62. A good case study of how this has attempted and failed occurred with the Transport Security Administration in the US. They have powers to search through people's luggage, for which they need to be able to open bags. However, many people also want to be able to lock their bags closed to avoid theft. The ingenious solution was to sell combination locks that would have a TSA-owned master key, so that in principle the TSA and only the TSA could simply unlock the lock using a key. This worked moderately well until someone was photographed holding a set of the master keys, which could then be replicated based on the image. The TSA lock system is now entirely unsecure, with criminals easily able to open the locks.

63. The US government looked carefully into the possibility of tackling encryption, but concluded that they will act '**without weakening our commitment to strong encryption**'. Papers from the US National Security Council argued that 'Overall, the benefits to privacy, civil liberties and cybersecurity gained from encryption outweigh the **broader risks that would have been created by weakening encryption.**' The same is true here in the UK.

64. Currently, there is legislation that allows operators to be required to maintain the ability to provide the content of communications unencrypted. The Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002, part 10 of the schedule. The sanction for breach consists of civil proceedings, and there is no record of any applications for such action. The IPB creates the same power in s189(4)(c).

65. It is unclear what would happen if a court were to be asked to take action against an operator who was unable to comply with this power because of the fundamental nature of their product. Any decentralised communications system is likely to render this clause impossible to comply with. In this case, there are two possible outcomes. The first is that no action would be taken, and the communications would continue to be undecryptable. Alternatively, action would be taken, which would potentially force an operator to cease providing their services legitimately in the UK. This latter options seems unlikely to be feasible, given the number of people who come into the country, largely as visitors, who may well have these apps on their phones or computer systems. The efforts to block twitter and other mechanisms in China have not been very successful, and are surely not the model we wish to follow.

66. **I would invite the Committee to recommend that the rules be clarified,** and in particular to make it clear what would happen in the event that a technical feature desired by the agencies cannot be achieved by an operator, or would make the service to vulnerable to cyberattack.

67. Clause 188 recreates a very broad power for the Secretary of State to require any steps of a telecommunications operator. As detailed in paragraph 24 above, **this power needs to be subjected to the safeguards present in the rest of the Bill.**

Costs of the proposals

68. The proposals in the CDB, which covered substantially less ground than those in the IPB, were estimated to cost £1.8 billion over 10 years. Our committee was very sceptical of these costs, describing them as 'not robust' and expressing a fear that 'this legislation will cost considerably more than the current estimates'.[444]

69. The CDB estimated benefits from the legislation as being between £5.0 and £6.2 billion over 10 years. We criticised these figures even more strongly, describing them as 'fanciful and misleading'.[445]

70. The overarching impact assessment provided by the Home Office for the IPB lists costs totalling £247 million over 10 years and no quantified benefits. It is remarkable in particular that the costs have come down so substantially in the intervening few years, despite the fact that very few of the powers requested in CDB have been removed, whereas a wide range of new powers have been added. **The committee should ask for clarity on why the claimed costs have been reduced so substantially, and how sure the Home Office are that the costs identified will cover all the costs involved,** in particular the costs of repaying all business costs, as identified in the impact assessment. This commitment should be on the face of the bill, as we recommended.[446]

[444] Report on the Draft Communications Data Bill, paragraph 262
[445] Ibid., paragraph 269
[446] Ibid., paragraph 263

Broader effects on the UK technology sector and innovation

71. In our report on the CDB, we were given considerable evidence which highlighted the consequences that piece of legislation would be likely to have had on UK businesses. We were, for example, told by the Internet Service Providers' Association that :

> *'The Draft Bill has the potential to put the UK at a competitive disadvantage and destabilise the market, with the UK seen as a less attractive and more onerous place to do business digitally, affecting both inward investment and services being made available.'*[447]

72. **The Committee might like to reiterate our conclusion, namely that the Government 'should bear in mind the importance of preserving their competitiveness, and minimising damage to the reputation of the United Kingdom as an attractive base for conducting business.'**[448]

21 December 2015

[447] Ibid., paragraph 274
[448] Ibid., paragraph 275

ICAEW—written evidence (IPB0044)

ICAEW welcomes the opportunity to comment on the Parliamentary Joint Committee on the Draft Investigatory Powers Bill Call for Written Evidence published by Parliament on 30 November 2015, a copy of which is available from this link.

This ICAEW response reflects consultation with the Business Law Committee which includes representatives from public practice and the business community. The Committee is responsible for ICAEW policy on business law issues and related submissions to legislators, regulators and other external bodies.

ICAEW is a world-leading professional accountancy body. We operate under a Royal Charter, working in the public interest. ICAEW's regulation of its members, in particular its responsibilities in respect of auditors, is overseen by the UK Financial Reporting Council. We provide leadership and practical support to over 144,000 member chartered accountants in more than 160 countries, working with governments, regulators and industry in order to ensure that the highest standards are maintained.

ICAEW members operate across a wide range of areas in business, practice and the public sector. They provide financial expertise and guidance based on the highest professional, technical and ethical standards. They are trained to provide clarity and apply rigour, and so help create long-term sustainable economic value.

Communications data involving certain professions

1. We welcome the opportunity to comment, as well as the Government's commitment to provide a clear legislative framework for surveillance activities.

2. We believe that maintaining trust in the professions is in the public interest. If such relationships of trust and confidence were to be threatened it may seriously undermine the public right of access to professional advice. The confidentiality of the advice provided by professionals is vital to the functioning of our legal and economic system. We therefore believe that the public interest would be better served by the introduction of primary legislation governing the protection of sensitive and confidential communications data, rather than a code of practice.

3. Confidentiality is a fundamental ethical principle to which accountants are required to adhere by domestic and international standards. Only in certain circumstances will the advice they offer be subject to legal professional privilege, but that does not make it any less sensitive. Therefore all of the concerns regarding sensitivity of confidential communications are relevant to accountants but also highly relevant to any individual who chooses to seek confidential professional advice.

4. We note that the special protections as drafted apply only to legally privileged information, banking records, MPs communications and relevant confidential

information as defined by the Police and Criminal Evidence Act, which in turn only protects personal records connected with physical/mental health and counselling matters. We think that this is too narrow and additional safeguards should be extended to all professions that have a duty of confidentiality, including accountants.

5. More generally we share concerns with many others around law enforcement access to an user a significant amount about an individual's private activities. This would include details about the nature and existence of a professional relationship which, in itself, could be highly sensitive.

18 December 2015

The Information Commissioner's Office—written evidence (IPB0073)

Executive Summary:

- The draft bill is far-reaching with the potential to intrude into the private lives of individuals. The case justifying the measures, the necessity for them, their proportionality and the adequacy of compensatory safeguards, must be subject to detailed scrutiny.
- Parliament has a responsibility to scrutinise these provisions, not simply as they stand in the bill but in the wider context of surveillance generally.
- The law must be kept under ongoing review, with provision for effective post legislative scrutiny. A 'sunset clause' could ensure that this happens.
- The value of communications data to law enforcement is understood and is also vital to the Commissioner's own enforcement work.
- Little justification is advanced for the need to retain data for twelve months and the definition of any retention period needs to be evidence based.
- The Information Commissioner's role in auditing retained communications data needs strengthening with obligations on CSPs to cooperate combined with sanctions if they do not; greater clarity on access to CSPs' records; provision for retention notices; and a requirement for the Information Commissioner to be consulted on any codes of practice affecting the Commissioner's duties. Safeguards in relation to non-UK CSPs need clarifying.
- Internet connection records can be revealing and strong justifications for intrusion are required including the reassurance of post legislative scrutiny.
- Examples of the need for bulk personal data set warrants are not persuasive since equivalent provisions already exist in statute. The established approach could be used for data sets of concern. Consideration should be given to exempting certain data sets involving sensitive personal data, such as those, for example, relating to health data.
- Safeguards surrounding equipment interference and protecting privileged communications need reconciling and strengthening.
- Notices requiring the removal of electronic protection should not be permitted to lead to the removal or weakening of encryption. This technique is vital to help ensure the security of personal data generally.
- The simplification and strengthening of oversight arrangements is welcome, but should not be overstated, particularly the role of a Judicial Commissioner. The IPC role will be vital including in improving transparency. The role must be independent and inspire public confidence. Reports should include the value of data to law enforcement outcomes so that continued need and justification can be assessed. The process for notifying individuals of any errors should be strengthened.

Introduction

1. The Information Commissioner has responsibility in the United Kingdom for promoting and enforcing the Data Protection Act 1998 (DPA) and the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations (EIR) and

the Privacy and Electronic Communications Regulations 2003, as amended (PECR). The Information Commissioner also has a more limited supervisory role under the Data Retention Regulations 2014 (DRR 2014) created under the Data Retention and Investigatory Powers Act 2014 (DRIPA).

2. He is independent from government and upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals and taking appropriate action where the law is broken. His activities also include providing advice on policy and other initiatives that engage information rights concerns.

3. This evidence will focus on those aspects of the draft bill that fall within the Information Commissioner's direct regulatory remit. It also covers the other aspects of the draft bill that have an impact on the privacy of individuals.

4. The Information Commissioner recognises that there are significant and ever developing challenges that law enforcement and security bodies face in fulfilling their role. These challenges are not limited to the threats themselves but also involve the changing technological means that may be used. The Commissioner recognises that the provisions in the draft bill are aimed at helping law enforcement and security bodies respond to these evolving challenges. But it is not sufficient to give wide ranging powers without very careful consideration of the justification, the pressing needs they are meant to address, the proportionality of the measures themselves, and adequacy of any compensatory safeguards. To fail to make such a balanced assessment risks eroding the very freedoms those measures are intended to protect. Respect for an individual's private life is one of our cherished freedoms.

5. The draft bill is welcome to the extent that it brings together disparate existing measures into a single legislative context with the opportunity for proper parliamentary scrutiny of the whole package.

6. Parliament has a significant role to play not only in scrutinising the case justifying such measures, their proportionality, and the adequacy of safeguards. It has an important role in considering these measures in the wider context of the ever increasing general surveillance of individuals. All of us leave digital footprints as we go about our everyday business, whether using a mobile phone, sending an email or text message, visiting a website, or checking social media. These digital footprints do not just show activities but can record our locations too. We feature increasingly on databases compiled in many different and specific contexts by both public and private sector organisations. There are significant features of the draft bill that touch on the lives of all citizens, not just those suspected of involvement in criminality.

7. There are also other forms of surveillance by public bodies. Examples include widespread automatic number plate recognition systems (ANPR) which results in an average of around 30 million records of the routine use of vehicles being collected every single day. These records are not linked to any suspicion of criminal activity, but they are nevertheless retained in a central database for a number of years.

Similarly, access to airline passenger name records for those who fly in or out of the UK can be extensive and largely unseen. Ally to this the extensive network of CCTV cameras and this technology's developing capabilities and there is an increasing danger that we are living in a society where few aspects of our daily private lives are beyond the reach of the state. This poses a real and increasing risk that the relationship between the citizen and the state is changed irreversibly and for the worse[449].

8. Parliament has a vital role in considering the draft bill not only on its own merits but also in the broader context of all these wider developments, many of which have evolved with little, if any, statutory underpinning - but always in the name of improving public security and the capabilities of those who are there to protect us.

9. Measures in the draft bill which require more extensive information to be retained, make that information available to others in different contexts than for which it was originally collected, and store it for prolonged periods, engage concerns about core data protection and PECR safeguards. These protections include appropriate transparency, individual control, purpose limitation, data minimisation and ensuring effective security measures. These protections are aimed at minimising information risk (such as unwarranted intrusion or the consequences of a security breach) and providing individuals with confidence that their information will be respected and safeguarded.

10. These protections are underpinned by Article 8 of the European Convention on Human Rights (ECHR) and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (the Charter). Article 8 of the Charter provides a specific right to data protection, emphasising its importance to citizens in the modern world. None of these provisions are absolute rights and all recognise the need to accommodate other important societal needs. Our own DPA has its provisions limited where there are statutory requirements, national security may be affected, or law enforcement purposes likely to be prejudiced[450].

11. Judgements of the courts now clearly reflect the importance of these protections, both at domestic[451] and European[452] level. These cases point to the importance of properly assessing and weighing the impact on the fundamental right to privacy and data protection. The new General Data Protection Regulation, recently agreed, will come into force in 2018 and will increase the potential of jurisprudence from the Court of Justice of the European Union (CJEU) impacting on data protection and the relationship with fundamental rights. From the existing case law it is clear that the following guarantees should be in place when personal data is being processed by national security bodies:

---

[449] see Information Commissioner's 2010 report to Parliament on the state of surveillance https://ico.org.uk/media/1042386/surveillance-report-for-home-select-committee.pdf

[450] See, for example, exemptions provided under DPA sections 28, 29 and 31.

[451] Secretary of State for the Home Department -v- David Davis MP and others [2015] EWCA Civ 1185

[452] Digital Rights Ireland (Advocate General's opinion) [2013] EUECJ C-293/12 (12 December 2013); also Maximilian Schrems v Data Protection Commissioner case (C-362-14)

- Processing based on clear, precise and accessible rules
- Necessity and proportionality with regard to the objectives pursued
- Existence of an independent oversight mechanism
- Effective remedies for the individual

12. Parliamentary scrutiny is an essential component not only when the legislative measures are considered initially, but also through regular detailed post legislative scrutiny and review. The Information Commissioner has previously recommended the inclusion of 'sunset clauses' to ensure that the threats the legislation is intended to address still exist, the measures are effective in addressing these, and the right balances are struck in practice. The draft bill is far reaching and has the power to affect the lives of all citizens to differing degrees. For these reasons, the bill should include a sunset clause or other provisions requiring effective post legislative scrutiny. This would ensure that measures of this magnitude remain necessary, are targeted on the right areas, and are effective in practice. To fail to make this provision risks undermining public trust and confidence. It will also enable the legislation to be considered in the light of the latest jurisprudence from the CJEU and European Court of Human Rights (ECHR)

13. The Information Commissioner's view on the key aspects of the draft bill that engage his statutory functions are set out below, followed by his comments on other provisions of the draft bill.

Communications Data

14. The amalgamation of a number of separate provisions relating to the retention of communications data within the one legal instrument is welcome, particularly some of the detailed provisions which previously existed in the Data Retention Regulations 2014 (DRR 2014) rather than in the primary legislation. There is still a reliance on codes of practice to provide additional details and safeguards. It is important that the likely content of these codes is available for scrutiny during the passage of the bill so that the whole regulatory framework including any limitations is clear.

15. The Information Commissioner does understand the value of communications data for investigatory purposes. He has first-hand experience of its evidential value in relation to his own enforcement and prosecution powers and it is important that he is specified in Schedule 4 as a relevant public authority. In particular the power to acquire communications data is essential to his work in prosecuting the unlawful obtaining and disclosure of personal data and tackling nuisance telephone calls and texts. The lack of this data would impair his ability to take action in areas of increasing public concern.

16. The concept of Communication Service Providers (CSPs) retaining data for longer than needed for their own business purposes and then making this available to specified bodies on request is carried forward from existing legislation. This approach is preferable to the creation of a central data centre where data could, in theory, be

transferred and held under state control. The period for retention remains at twelve months though there is little evidence provided explaining why this is the appropriate period. The justification for this period should be made clear, especially as it should be possible to provide evidence of the number of such requests and their law enforcement outcomes based on current arrangements.

17. The Information Commissioner has built up his own experience of exercising his current audit functions under DRR 2014 in respect of retained data and has identified areas where the provisions surrounding this can be improved.

18. The Information Commissioner will be required under clause 182 to audit the integrity, security and destruction of retained data. This aligns with his current role under the DRR 2014. As currently drafted, the draft bill does not require CSPs to cooperate with the Information Commissioner's audits on the integrity, security or destruction of data held under a relevant notice from the Secretary of State. The existing position under the DRR 2014 facilitates this through the retention notices given to CSPs and their compliance with the Retention Code of Practice. Putting a duty on the Information Commissioner to undertake an important oversight role without the accompanying powers in primary legislation to fulfil this duty is a deficiency that needs remedying. For example, under section 40A of the DPA, the Information Commissioner has the power to serve an assessment notice on a government department or NHS body in order to undertake a compulsory audit.

19. Whilst this has not prevented the Commissioner from complying with his obligations to date there have been challenges from CSPs around the extent of the Commissioner's powers. Putting a duty on CSPs to cooperate could also make clear it covers all 'retained' data covered by a retention notice including data retained in CSPs' disclosure systems, another area of query. It is our experience, from our wider audit role under the DPA, that organisations cooperate more readily where we have a clear statutory power of audit. Such provisions could also include sanctions for failing to cooperate. The draft bill could also clarify that the offence provisions at section 59 of the DPA which cover the confidentiality of information provided to the Information Commissioner also extend to the performance of his duties under clause 182.

20. The draft bill should also provide for the Information Commissioner to be directly notified about retention notices being issued, varied and revoked. Given that the Information Commissioner's powers of audit relate to the Secretary of State's retention notices there should be a proactive duty on the Secretary of State to inform the Information Commissioner.

21. Schedule 6 of the draft bill sets out the ability of the Secretary of State to issue relevant codes of practice. The current Retention Code sets much of the practical details surrounding the retention of data by CSPs and the Information Commissioner's role in supervising aspects of their activities. Given the

Commissioner's interest in this code he should be added to the list of bodies with whom the Secretary of State must in particular consult when producing a code[453] .

22. The importance of the arrangements that are set out in the Retention Code are illustrated by current provisions in the DRR 2014 detailing the way in which communications data are to be retained by CSPs.

23. Retaining more data for longer inevitably engages concerns about the security of the retained data. Regulation 7 of the DRR 2014 currently requires CSPs to hold data securely and specific security arrangements for the retention of data by CSPs are set out in chapter 6 of the Retention Code. This also provides for the Home Office to include specific security requirements in data retention notices and to provide security advice and guidance to all CSPs who are retaining data. The Retention Code envisages retained data being kept in a dedicated retention and disclosure system which is securely separated from a CSP's business system. However the Retention Code does provide for an alternative, and data may be retained in business or shared systems subject to specific security safeguards being agreed with the Home Office.

24. Whilst it may be possible to ensure that normal business systems holding retained data have the appropriate security safeguards in place such systems are, by their nature, aimed at facilitating wider business use with greater levels of access. This may pose more of a challenge not only for CSPs to ensure appropriate security but also for the Information Commissioner to audit. Ensuring there is a requirement, either on the face of the legislation or in a subsidiary code of practice that requires the data to be retained separately from normal business systems may help reduce security risks. This is all the more important given retention of internet connection records (ICRs).

25. Clause 182 requires the Commissioner to audit CSPs who are complying with retention notices under Part 4 of the draft bill. Clause 79 makes clear that persons outside the UK can receive such notices and must have regard to these. It is not clear whether this would also include complying with the safeguards in clause 182 and, if so, how this would be achieved in practice with a CSP in another jurisdiction. This needs clarifying as, otherwise, important compensatory safeguards may not be available in practice.

26. One potentially welcome feature of the draft bill is the filtering mechanism proposed at clause 51. If this mechanism is effective this could reduce privacy intrusion such as when trying to resolve IP addresses. However how this would work in practice would require some attention and close review by the Investigatory Powers Commissioner (IPC) to ensure that it is achieving its aims and not being used in inappropriate ways.

Internet Connection Records

27. One new feature in the draft bill surrounds the requirement on CSPs to retain Internet Connection Records (ICRs). Although these are portrayed as conveying

[453] See schedule 6 section 5(2)

limited information about an individual they can, in reality, go much further and can reveal a great deal about the behaviours and activities of an individual. Such records would show particular services that are connected to and this could be a particular website visited although not the pages within them. This could lead to a detailed and intrusive picture of an individual's interest or concerns being retained and then disclosed. There is also increased risk to all individuals if such retained data are subject to a security breach and that detailed picture of their interests and activities becomes available to third parties. This could lead to unintended consequences and again reinforces the need for specified security requirements for CSPs to safeguard against this risk.

28. Retaining ICRs is an area where there needs to be strong justification and if this is made on the basis of an assertion of need in advance of a power being given then there needs to be effective post legislative scrutiny to judge the magnitude and nature of the records retained and the use that was made of these in practice including law enforcement outcomes.

29. There are challenges in resolving IP addresses down to particular identifiable individuals which may make such data of less value in practice. It is understood that in 2014 Denmark repealed its provisions that are similar to the draft bill as they were unable to achieve their objectives in practice. It is not sufficient for the IPC to report on the working of the arrangements; it is the use of the information and its value that is the indicator of whether such intrusion is necessary and proportionate. This information would need to be provided as part of any post legislative scrutiny.

30. The requirement to retain ICRs also adds another dimension to the Information Commissioner's role extending the records that must be supervised. At present the Commissioner receives specific grant in aid from the Home Office to undertake his functions under the DRR 2014. That is based upon a predicted number of audits and a dedicated audit team has been created for this purpose. If the nature or number of records retained increases this will require appropriate funding for this additional work to ensure the audit controls remain an effective safeguard. This will also be true if there are requirements to audit CSPs providing services from outside the UK.

Bulk personal dataset warrants

31. The provisions in the draft bill around the acquisition of bulk personal data sets require particular scrutiny. These provisions are limited to the security and intelligence services. The examples given in the Guide to Powers and Safeguards refer to telephone directories and the electoral roll. These datasets are already available to various agencies often under specific statutory provisions. For example, Schedule 1 of the Counter-Terrorism Act 2008 amends the Representation of the People (England and Wales) Regulations 2001 to require the supply of the full electoral register to the security services. The relevant specific legislation can be amended if there are issues around any limitation affecting availability to the security and intelligence services as this amendment demonstrates. The examples in the Guide seem particularly inappropriate given the existing availability of these datasets

and others, including vehicle keeper and driver data, to conventional law enforcement bodies.

32. There are also limitations on the applicability of the DPA where this may affect national security (s.28) with a Minister of the Crown being able to provide a conclusive certificate to that effect only challengeable by way of judicial review. This can mean that data sets are already disclosed, such as, for example, congestion charging data held by Transport for London to the Metropolitan Police. It is not clear why existing provisions are considered insufficient. A clearer justification needs to be made of the types of data that are not currently available under existing provisions and why warrant provisions are necessary. These warrant powers should not be available in addition to existing statutory access arrangements.

33. Given the increasing amounts of personal data generated and held in data sets this could be a particularly far reaching and intrusive provision. Whilst the safeguards surrounding authorisation are welcome, there may be some data sets that should be exempted. An obvious example is health data where there are other substantial public policy reasons why such data should not be available in bulk. There is increasing centralisation of records such as with the Care.data programme and other efforts to create significant national level collections of health related information.

34. There are no arrangements for auditing the acquired data and this omission should be rectified. This could include ensuring that only information of value is retained, with measures implemented to delete personal data that is not of interest.

Equipment Interference

35. Equipment interference has the potential to be intrusive and it could also damage the very systems subject to interference with unforeseen consequences. It is not clear why a differential approach to the warrant authorisation process has been adopted, with the Secretary of State having a role in certain cases but chief law enforcement officers in others. The same is true of with modifications where a Judicial Commissioner reviews law enforcement bodies but not intelligence agencies. There should be a consistent and appropriately robust approach adopted.

36. There are also differences in the way safeguards are applied. Clause 85 sets out specific safeguards for Members of Parliament but these are not extended to others who are involved in privileged communications protected elsewhere in the draft bill. There should be consistency of approach.

Maintenance of Technical Capability-Removal of Electronic Protection

37. Clause 189 permits the Secretary of State to impose obligations relating to the removal of electronic protection applied by a relevant operator to any communications or data. This could be a far reaching measure with detrimental consequences to the security of data and safeguards which are essential to the public's continued confidence in the handling and use of their personal information.

38. If the possible obligations surround the weakening or circumvention of encryption then this is matter of real concern. The Information Commissioner has stressed the importance of encryption to guard against the compromise of personal information. Weakening encryption can have significant consequences for individuals. The constant stream of security breaches only serves to highlight how important encryption is towards safeguarding personal information. Weakened encryption safeguards could be exploited by hackers and nation states intent on harming the UK's interests. This evidence has already pointed to potential concerns, at paragraphs 23-24, about retained communications data being held on normal business systems and the increased challenges of ensuring appropriate security. These concerns would increase still further if necessary electronic protections were weakened or removed.

39. The practical application of such requirement in the draft is unclear in the draft bill and the accompanying Guide to Powers and Safeguards does not provide specific details to enable the full extent of the provision to be assessed.

40. Sub-clause 190 (8) requires that the existence of any such a requirement is not disclosed so there is no transparency around the existence of measures that could affect encryption of an individual's information. This clause and Clause 191 do provide for an operator to ask the Secretary of State to review the requirement and the IPC and Technical Advisory Board need to be consulted. However, the Secretary of State can still proceed with the requirement irrespective of any contrary view expressed by either body. This seems a significantly weaker position than other aspects of the draft bill that requires an actual approval.

Oversight Arrangements

41. Central to the proposed oversight arrangements is the creation of the IPC bringing together existing functions. The Information Commissioner welcomes this as the existing landscape is complex. He took the initiative in producing a 'surveillance roadmap' to set out the various functions to try to explain the different powers and responsibilities of the various commissioners. The proposals in the draft bill are a welcome simplification. It is important that the IPC receives the necessary funding to provide the high level of public reassurance this role is meant to provide. It is also important that the IPC is independent.

42. It is important that commissioners with a corresponding interest in issues do cooperate and we have experience of setting out more formal arrangements such as working with Interception of Communications Commissioner to develop a memorandum of understanding over the reporting of security breaches by CSPs. There will be further scope for sensible cooperation, given the supervisory role of the IPC, to ensure that matters that also affect data protection compliance concerns or the duties under clause 182 are referred to the Information Commissioner.

43. Ensuring individuals have effective rights of redress where powers are used incorrectly must be an essential component of the regulatory framework. The draft

bill includes provisions that should help improve on the existing position such as the IPC examining errors and the impact of these on individuals. These are then referred to the Investigatory Powers Tribunal to consider whether an individual affected should be contacted. This still leaves a significant discretion in the hands of these two bodies. Making individuals aware of errors unless there are significant reasons not to do so, such as prejudicing an ongoing or planned operation/investigation, should be the norm.

44. Another significant difference from the current landscape is the inclusion of Judicial Commissioners as part of the IPC arrangements. They represent what has been described as a 'double lock'. Clarity is important when describing this arrangement. The Judicial Commissioners review a decision, primarily one made by the Secretary of State, through applying judicial review principles to that decision such as the reasonableness of the action. This is not quite the same as approving an application on their own initiative and from first principles. Whilst this is a useful additional oversight role, it is not the same as a direct application to a judge for a warrant. A decision refusing to approve a warrant may also be subject to review on application to the IPC by the Secretary of State who may then overrule that decision. To refer to this process as a 'double lock' may be overstating this safeguard as it is essentially a more limited review process and even then subject to appeal.

45. It is important that there is appropriate separation of roles within the IPC to ensure that its oversight mechanisms are not perceived as being compromised by its authorising role, or the Judicial Commissioners falling within that framework. There must be no impression of 'marking their own work'. The IPC must provide annual reports but the mandatory content of that report, specified at clause 174, does not include anything around the value of that data to the bodies who gain access to data in terms of results achieved thereby. This is essential to judging whether measures are necessary and strengthens the need for effective post legislative scrutiny. Transparency would also be aided by information revealing the extent of the use of powers under the legislation. This may need to stop short of revealing the organisations who have received warrants or notices but information could be provided on the number of warrants and notices that have been served or are active at any one time. Expanding the breadth of the IPC's reports will also be a welcome step towards further increased transparency, a prerequisite for helping maintain public trust and confidence.

Conclusions

46. The draft bill provides an important opportunity for full consideration of the range of investigatory powers provided to public bodies and the overall effects on citizens. Ensuring that these powers are put on a clear and predictable legal basis is essential. The inclusion of mechanisms to ensure that proper processes are followed with appropriate review is vital. The draft bill includes some welcome features. But all these need to be weighed against a clearly articulated pressing need and rationale showing how and why the measures are necessary to achieve these. More needs to

be done such as around retention periods for communications data, the need for all internet connection records, and range of personal data sets available under warrant.

47. It is also essential that there is appropriate transparency in the operation of arrangements and the reports of the IPC will have an important role to play. But there also needs to be more formal post legislative scrutiny of the need for measures with evidence provided of the actual outcomes resulting from the measures. Only then can the continued need and proportionality be judged. Including a sunset clause should ensure this happens.

48. Safeguards also need further attention including strengthening the Information Commissioner's powers where these act as compensatory safeguards placing specific duties on CSPs to cooperate with him and prescribing sanctions for those who do not. There are also important additional safeguards that could be introduced to reduce the risk of security breaches in relation to retained data. Similarly powers to require the removal of electronic protection must not extend to removing or weakening encryption which plays an essential role in helping ensure the security of personal information.

49. The oversight provisions including review by a Judicial Commissioner are a positive step, but fall short of full judicial approval of measures. There can also be a strengthening of the circumstances where individuals are made aware of errors that have affected them giving them the opportunity to take their own action and hold authorities to account. Expanding the range of matters that the IPC must report on to include a review of the overall operation of the regime would also be a welcome step towards improved transparency.

Christopher Graham
Information Commissioner

18 December 2015

The Institute for Human Rights and Business (IHRB)—written evidence (IPB0094)

1. The Institute for Human Rights and Business (IHRB) welcomes the opportunity to submit written evidence to this inquiry. We would also like to thank the Joint Committee for convening the oral evidence sessions during the past few weeks, which we have found very informative.

2. This submission is a response to the call for written evidence[454] published by the Joint Committee and the some of the questions posed therein. Our comments draw on IHRB's previous research in Myanmar developing a "Rights Respecting Model for Communications Surveillance through Lawful Interception and Government Access to User Data".[455] This model sets out important principles for each step of developing and implementing a communications surveillance legal framework that protects and respects human rights, and will shortly be published as an IHRB Occasional Paper.

3. This submission focuses on some outstanding questions arising from provisions in the draft Bill that can benefit from further clarification and scrutiny in the Joint Committee's forthcoming report and recommendations to the Houses in February 2016:

- Clarifying the definitions of telecommunications services and systems.
- Further examination of the compatibility of bulk powers provided for in the draft Bill with human rights standards, including bulk personal datasets.
- Clarifying the aim and feasibility of obliging telecommunication operators to retain Internet Connection Records (ICRs).
- Clarifying the procedure by which overseas operators are expected to comply with the extraterritorial provisions in the draft Bill, particularly provisions only concerning people and communications based outside of the UK, including bulk interception and bulk equipment interference.
- In addition, we provide recommendations to strengthen the oversight mechanisms provided for in the draft Bill and access to remedy.

4. Definition of Telecommunications Services and Systems

4.1 In Part 9, Clause 193 (Telecommunications Definitions) of the draft Bill, telecommunications services and systems are defined as:

(11) "Telecommunications service" means any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service).

(12) For the purposes of subsection (11), the cases in which a service is to be taken to consist in the provision of access to, and of facilities for making use of, a telecommunication system include any case where a service consists in or includes facilitating the creation, management or storage of

[454] http://www.parliament.uk/documents/joint-committees/draft-investigatory-powers-bill/ipb-call-for-evidence.pdf
[455] See, http://www.myanmar-responsiblebusiness.org/pdf/SWIA/ICT/Executive-Summary-and-Recommendations.pdf (p35)

communications transmitted, or that may be transmitted, by means of such a system.

(13) "Telecommunication system" means a system (including the apparatus comprised in it) that exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro- magnetic energy.

4.2 With the development of the "Internet of things" and "big data", in the near future this definition could encompass a much wider range of companies that rely on Internet services to deliver products and services. The issue of surveillance is no longer confined to the Information and Communications Technology (ICT sector) and is likely to become a cross-sector issue that impacts a wider range of companies, such as automobile and energy.

4.3 It is unclear whether the current definition includes devices that generate data relating to individuals that may not involve communication between two people, but instead machine-to-machine communication. For example, automated infrastructure involved in the collection of data relating to cars, wearables (such as fitness) or energy smart meters. Could the Committee envisage situations in which companies generating datasets relating to geo-location (such as Internet-connected cars) or energy use (such as gas/electric smart meters) would be served with a data retention notice? Are these companies and the public aware that this personally identifying information may be accessible to the police and intelligence and security services as a matter of course, including the collection of bulk personal datasets?

5. Bulk Powers (including Bulk Personal Datasets)

5.1 Publicly avowed for the first time in the draft Bill are many bulk collection capabilities: bulk interception of communications, bulk acquisition of communications data, bulk personal datasets and provisions for bulk equipment interference.

5.2 Although the bulk collection capabilities are publicly avowed, we believe that the case has not been made for retaining bulk powers, in particular bulk personal datasets and bulk equipment interference (see section 7). We believe there are still many outstanding questions as to whether collecting and retaining communications in bulk is compatible with the protection of the right to privacy, as outlined in Article 17 of the International Covenant on Civil and Political Rights (ICCPR), Article 8 of the European Convention of Human Rights and Article 8 of the Human Rights Act.

5.3 Under Article 17 of the ICCPR, any restrictions on the right to privacy must not be either unlawful or arbitrary. In the recent report, "The Right to Privacy in the Digital Age," presented to the UN Human Rights Council in June 2014, the UN High Commissioner for Human Rights explains these restrictions further[456]:

(i) "**Unlawful**": A restriction is "unlawful" when it is not authorised by States on the basis of national law specifically authorising interference. The national law must be sufficiently accessible, clear and precise and also must not conflict with other

[456] See Report of the Office of the United Nations High Commissioner for Human Rights A/HRC/27/37 Right to Privacy in the Digital Age para 21-23. Available at: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

provisions of the ICCPR, such as the prohibition on discrimination or the country's own constitution or

(ii) "**Arbitrary**". The protection against "arbitrary interference" means that the interference should be **reasonable** in the particular circumstances. It must be in **proportion to the aim** and the least intrusive option available to accomplish the aim and be **necessary** in the circumstances for reaching a legitimate aim.

5.4 The same report highlights that the onus is on the relevant authorities to show that proposed limitations on the right to privacy are connected with a legitimate aim. The limitation must also be shown to have some chance of achieving that goal while at the same time not being so overly restrictive that the restriction makes the exercise of the right meaningless. Where the limitation does not meet these criteria, the limitation would be unlawful and/or the interference with the right to privacy would be arbitrary.[457]

5.5 Communications surveillance must be limited to that necessary to achieve a legitimate aim and use the means least likely to infringe rights – it must be both necessary and proportionate. The UN Special Rapporteur on the promotion and protection of fundamental freedoms while countering terrorism stated in a 2014 report, *"With targeted surveillance, it is possible to make an objective assessment of the necessity and proportionality of the contemplated surveillance, weighing the degree of the proposed intrusion against its anticipated value to a particular investigation."*[458]

5.6 Part 7, Clause 151 of the draft Bill provides that bulk personal datasets are authorised by class based warrants - these warrants do not name individuals or addresses but rely on generalised categories of people or places. This means that the communications of potentially millions of people not suspected of any crime will be collected and stored. This is acknowledged in the draft Bill; for example in the Draft Investigatory Powers Bill: Guide to Powers and Safeguards, Bulk Personal Datasets are described as, *"sets of personal information about a large number of individuals, the majority of whom will not be of any interest to the security and intelligence agencies."*[459]

5.7 An objective assessment of the necessity and proportionality of the contemplated surveillance is stated as a core part of the authorisation process in the draft Bill. However, the broad use of bulk powers and class based warrants which are likely to collect personal information of individuals not suspected of any crime and in such volume makes the necessary and proportionate test extremely difficult, if not impossible to conduct.

5.8 UN experts have indicated serious concern about communications surveillance that is authorised on such a broad and indiscriminate basis. Actions of this scope are seen as running counter to the whole core concept of the protection of privacy that requires justification for intrusions on privacy to be made on a case-by-case basis.[460]

---

[457] Ibid, para 23.

[458] See: UN General Assembly A/69/397 23 September 2014, para 7. Available at: http://s3.documentcloud.org/documents/1312939/un-report-on-human-rights-and-terrorism.pdf

[459] Draft Investigatory Powers Bill: Guide to Powers and Safeguards, p31, para 69.

[460] See the Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/23/40 (para 54) 17 April 2013. Available at: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf and the Report of

6. **Internet Connection Records (ICRs)**

6.1 There are outstanding questions regarding the definition of ICRs, whether collection will achieve the stated aim, whether it is technically feasible to obtain them and how large the associated costs will be.

6.2 During a recent session of the Science and Technology Committee[461], witnesses from the ICT Sector expressed concern about how the separation of content and communications data in this context could technically happen. A recent report suggested that it would take at least 18 months to determine this technical feasibility and the associated costs, which are expected to be significantly higher than the £174 million the Government has set aside to underwrite costs incurred by the industry over 10 years.[462]

6.3 Companies required to retain their customer ICRs for twelve months will be served with a Data Retention Notice issued by the Secretary of State, when it is deemed "necessary and proportionate" to do so. We believe the circumstances by which it would be necessary and proportionate to retain all user ICRs has not yet been specified.

6.4 Transparency is extremely important in order to build trust among stakeholders. Companies should be able to be transparent with users about the collection, storage and access of ICRs and should not be prevented from including any requests from government agencies for datasets in their transparency reports.

7. Extra-territorial applications of provisions in the draft Bill and compliance of overseas operators

7.1 The Draft Investigatory Powers Bill: Guide to Powers and Safeguards states that the draft Bill *"places the same obligations on all companies providing services to the UK or in control of communications systems in the UK. However, the draft Bill only provides for those obligations to be enforced through the courts against overseas companies in respect of communications data acquisition and (targeted and bulk) interception powers. The draft Bill will include explicit provision to take account of any potential conflict of laws that overseas companies may face."*[463]

7.2 Part 3 of the draft Bill focuses on **authorisation for obtaining communications data**. Clause 46 provides that communications data will be acquired by serving a notice on a telecommunications service provider. Clause 50 states that telecommunications service providers have a duty to comply with the notice. Clause 69 focuses on the extraterritorial application of Part 3, and that notices can be served on telecommunications operators based outside of the United Kingdom.

---

the Office of the United Nations High Commissioner for Human Rights A/HRC/27/37 Right to Privacy in the Digital Age (para 27). Available at: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

[461] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/oral/24378.html

[462] http://www.theguardian.com/world/2015/dec/15/bt-vodafone-o2-ee-3-cost-feasibility-snoopers-charter?CMP=Share_iOSApp_Other

[463] The Draft Investigatory Powers Bill: Guide to Powers and Safeguards, p30, para 68.

7.3 The issue of serving extraterritorial notices is controversial, as can be seen, for example, in the case Microsoft vs. Ireland.[464] The Independent Reviewer of Terrorism Legislation, David Anderson, looked at the issues surrounding international data sharing in his June 2015 report, A Question of Trust and concluded, *"there is no immediate solution in sight"*[465](11.28). With this current perceived stalemate, we do not believe that the draft Bill provides any further clarity on how to manage the issue of obtaining communications data from overseas companies to assist with a specific investigation or a specific operation.

7.4 Part 1, Clause 7 of the draft Bill provides for **restrictions on requests for overseas interception** that is targeted. This clause provides that a mutual assistance warrant, under an EU mutual assistance instrument or in accordance with an international mutual assistance agreement, needs to be in place before a request for interception can be made to authorities outside the UK.

7.5 David Anderson's report noted, "*there is little dispute that the MLAT [Mutual Legal Assistance Treaty] route is currently ineffective*" and the "*MLAT route does not address intelligence needs*."[466]

7.6 The Prime Minister's Special Envoy on Intelligence and Law Enforcement Data Sharing, Sir Nigel Sheinwald, put forward proposals in a June 2015 briefing to strengthen Government to Government co-operation, reforming the MLAT process[467] (which has been supported by many overseas companies[468]) and building a new international framework for data sharing. We ask the Joint Committee to advocate for the publication of this report, which may address some of these concerns and gaps in the draft Bill.

7.6 The provisions for bulk interception and bulk equipment interference warrants are only applicable for people and communications outside of the UK[469], so it is likely this will involve almost exclusively telecommunications operators based outside of the UK. While it is clear from the draft Bill that a mutual assistance warrant is required for targeted interception, it is unclear what kind of warrant is needed for bulk interception and bulk equipment interference.

7.7 It is also unclear at which point overseas companies would be expected to comply with bulk equipment interference. Would companies be expected to comply at the point of sale of devices or equipment, or perhaps during periods where customers have brought equipment to the company for repairs?

---

[464] http://digitalconstitution.com/

[465] https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf

[466] See, A Question of Trust (2015) 11.26

[467] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/438326/Special_Envoy_work_summary_final_for_CO_website.pdf

[468] https://www.reformgovernmentsurveillance.com/

[469] See provisions for Bulk interception warrants: Part 6, Chapter 1, Clause 107 (f) and Bulk Equipment Interference: Part 6 Chapter 3, Clause 145 (4)

7.7 Therefore, further clarity is needed on what is expected of overseas companies and the mechanisms through which this assistance would be requested in order to determine whether this provision is legal, necessary or proportionate.

8. Oversight and Remedy

8.1 Consideration should be given to permitting a confidential public interest advocate, for example an independent human rights expert, to be part of the Investigatory Powers Commissioner (IPC's) staff to ensure that appropriate consideration is given to the human rights implications of requests. This is particularly important given the high degree of secrecy of authorisation processes that relate to national security.

8.2 Third parties, including companies, should have the ability to bring information to the IPC where relevant, if they have evidence of surveillance powers being misused.

8.3 In cases where surveillance powers are misused, either intentionally or otherwise, there should be redress and remedy. But individuals need to know whether they have been subject to surveillance in order to bring a complaint to the Investigatory Powers Tribunal (IPT) and seek access to remedy.

8.4 It is understood that there will be times when individuals cannot be notified that they are under surveillance as doing so could jeopardise the surveillance itself. However, notifying individuals if they have been the subjects of surveillance is an important element of access to remedy for those who may have been subject to illegal surveillance. At a minimum, users should be notified that their communications have been subject to surveillance when the surveillance is complete. Such a provision is absent from the draft Bill.

8.5 The legal framework should set out the circumstances under which there may be a delay in individuals being notified that they are under surveillance. When individuals are informed that they have been the subjects of surveillance they should also be informed of the procedure for filing a complaint with the IPT if they wish to do so.

About IHRB

IHRB is a global centre of excellence and expertise (a think & do tank) on the relationship between business and internationally recognised human rights standards.

We work to shape policy, advance practice and strengthen accountability to ensure the activities of companies do not contribute to human rights abuses, and in fact lead to positive outcomes.

IHRB prioritises its work through time-bound programmes that can have the greatest impact, leverage and catalytic effect focusing on countries in economic and political transition, as well as business sectors that underpin others in relation to the flows of information, finance, workers and/or commodities.

21 December 2015

Interception of Communications Commissioner's Office—written evidence (IPB0101)

Summary of Points for the Committee to Consider

- We have concerns with the aggressive timeline for the Investigatory Powers Bill (hereafter the "IP Bill"). There should be a review provision included in the IP Bill to enable the legislation to be re-visited regularly by the Government and revisions to take place in light of experience, especially given the fact that communications technology is ever changing.
- The oversight provisions in Part 8 of the IP Bill require significant enhancement in order to prescribe properly the legal mandate and functions of the "world-leading oversight body" which the Government is seeking to create. 3 of the 6 elements of our oversight wish-list have been partly addressed and the remaining 3 have not been addressed by the clauses. This section of our evidence submission provides a number of key recommendations.
- Clause 171 is a paradox which requires substantial re-drafting and clarification to ensure that a) the delineation of responsibility between the Investigatory Powers Commissioner and the Investigatory Powers Tribunal (hereafter "the IPT") is clear and, b) individuals are able to seek effective remedy.
- Clause 8 (offence of unlawfully obtaining communications data) could have the unintended consequence of undermining the open and co-operative self-reporting of errors and contraventions currently undertaken. There is a real danger that this provision will reduce accountability and individuals' and public authorities' co-operation with our investigations into errors and contraventions.
- Is it desirable to have the same body responsible for authorising investigatory powers and undertaking the post facto oversight of the exercise of those powers? If so, the judicial authorisation and oversight elements of that body must be operationally distinct.
- There appear to be a number of clauses which provide exceptions for national security or which exempt the intelligence agencies from key safeguards (e.g. clauses 47(2), 47(3), 60(2), 60(3) and 61). Are these exceptions, especially the combined effect, justified?
- The Government has not taken the opportunity to bring all of the investigatory powers used by public authorities into the IP Bill. The result is a lack of clarity and inconsistency in application and approval procedures.
- The IP Bill also curiously prescribes different authorisation and modification procedures for targeted equipment interference warrants made on behalf of the intelligence services (or Chief of Defence intelligence) to those made on behalf of law enforcement. The different procedures are confusing and it is not clear on what basis they are justified.

Background

1. Thank you for inviting the Rt Hon. Sir Stanley Burnton, Interception of Communications Commissioner and Joanna Cavan, Head of IOCCO to give oral evidence to the Committee on 2nd December 2015. That session focused mainly on the proposals for Judicial Commissioners in the IP Bill.

2. At the request of the Committee we are providing follow up evidence concerning our "oversight wish-list", published on 2nd November 2015. In addition we thought it might be helpful to highlight to the Committee a number of other matters we think important which have not so far been debated in detail during the evidence sessions.

Investigatory Powers Bill Timeline

3. An incredible amount of work has been undertaken by the Government to get the IP Bill to this stage. The IP Bill is a complicated and very significant piece of legislation. A number of the investigatory powers provided for in the IP Bill have been exercised in the past with little or no transparency under vague statutory frameworks and as such they have never before been debated publicly. We welcome the Government's efforts to put these powers on a clearer statutory footing. However, we do have concerns about the aggressive timeline for the IP Bill to be debated and scrutinised.

4. It is important for the public to understand fully the privacy implications of this legislation which enables highly intrusive conduct to be undertaken. The public authorities and those impacted by the conduct will have to live with the operational consequences of this legislation for some time to come. Therefore the detail has to be right. We need to ensure that the legislation satisfies the rule of law, provides enhanced safeguards to increase accountability and transparency and provides the public authorities with the powers they need to counter threats to our national security, to prevent and detect crime and ultimately to protect the public.

5. Unfortunately time has not allowed for us to examine in detail all of the clauses and their likely consequences in this extensive piece of legislation or to submit detailed written evidence to the Committee. We are aware that a number of other key stakeholders have made the same point. As a result we have tried in this submission to concentrate on matters which have not yet been raised or debated publicly by others. A number of witnesses to the Committee have suggested that there should be a review provision included in the IP Bill to ensure that the legislation is re-visited regularly. This is a sensible proposition, first due to the short timeline provided for scrutiny and secondly due to the fact that communications technology is ever changing. We anticipate the need to regularly revise the legislation in light of experiencing new technologies, the trends in uptake and use.

6. To save repetition we would like to signpost the Committee to the issues highlighted in our detailed written evidence[470] to David Anderson QC's Investigatory Powers Review. Our evidence addressed the effectiveness of the current statutory oversight arrangements, the safeguards to protect privacy, the case for amending or replacing legislation and the statistical and transparency requirements that should apply. Many of the issues highlighted were addressed in the Review's report (A Question of Trust) and consequently have flowed into the IP Bill clauses.

7. We also recognise that a number of other experts and key stakeholders have raised concerns (and submitted written evidence) to the Committee on, for example, the clauses relating to thematic interception warrants, modifications to thematic warrants, and the principle of judicial review. We do not seek to repeat those points in our submission, but deem those concerns worthy of serious consideration by the Committee. We also make the point that we are not best placed to comment on the clauses that cover areas outside of our current oversight remit (e.g. bulk personal datasets, equipment interference etc) and we hope that the other Commissioner bodies that oversee those areas will submit evidence on the legitimacy and adequacy of those powers and safeguards.

Oversight wish-list

8. On 2nd November 2015 we published a wish-list containing 6 elements that we thought the IP Bill must contain in order to modernise and strengthen the current oversight of surveillance powers. The elements in our wish-list are set out below along with commentary on whether the IP Bill addresses sufficiently each element. In summary 3 of the elements of our wish-list have been partly addressed and the remaining 3 have not been addressed.

a. A single independent public facing oversight body – We support fully a single unified body with responsibilities for surveillance oversight. This will present an opportunity to streamline the oversight landscape, to put all of the oversight responsibilities on a statutory footing, to bridge some of the identified gaps and address the overlaps. The body must be independent, have an appropriate legal mandate and be public facing to promote greater public confidence.

   Partly addressed – We welcome the creation of a single Investigatory Powers Commission to replace the three current RIPA Commissioner bodies. However the oversight clauses in Part 8 of the IP Bill require substantial re-drafting in order to deliver what the Home Secretary has described as "world leading oversight". In particular -

   - **Investigatory Powers Commission** (absent from clauses) - There is no mention of the "Commission" in the IP Bill. The clauses are only concerned with the creation of the Investigatory Powers Commissioner and the Judicial Commissioners (hereafter the

[470] http://www.iocco-uk.info/docs/2014-12-5(2)%20IOCCO%20Evidence%20for%20the%20Investigatory%20Powers%20Review.pdf

"Judicial Commissioners"). There is no clear legal mandate for the oversight body and the clauses do not reflect the breadth of skills required to complement the Judicial Commissioners and ensure the oversight is effective. The reality is that the Judicial Commissioners will only be performing a very narrow part of the oversight – the prior authorisation of some of the more intrusive investigatory powers. The bulk of the oversight will actually be carried out by inspectors and staff within the Commission who need a clear legal mandate to require information from public authorities, to launch and undertake audits, inspections, inquiries, investigations and react in real time when non-compliance or contraventions of the legislation are discovered during an inspection. There are examples of oversight bodies created as separate "Commissions", e.g. section 9 of the Police Reform Act 2002 created the Independent Police Complaints Commission as a body corporate. We believe this legal structure provides an appropriate model for the Investigatory Powers Commission, with statutory functions vested in the body corporate as well as the Judicial Commissioners.

- **Appointment of Commissioners** (clauses 167 & 168) – It is inappropriate for the Judicial Commissioners to be appointed by the Prime Minister as this dilutes public confidence and independence. The more modern arrangement and increasing standard internationally is for judicial appointments to be made by an independent body rather than the executive. It would be more appropriate for the Judicial Commissioners to be appointed by the Judicial Appointments Commission in consultation with the Lord Chief Justice. In a similar vein Judicial Commissioners should not be removed from office without the agreement of the Lord Chief Justice.
- **Funding, Staff and Facilities** (clause 176) - It is inappropriate for the Secretary of State to be responsible for determining what staff, accommodation, equipment and other facilities are necessary for the carrying out of the Judicial Commissioners' functions, particularly because those Commissioners will be reviewing the Secretary of State's authorisations. Again, the more modern arrangement and increasing standard internationally is for is for the judiciary to determine the resources (including personnel) they require, rather than the executive, and to determine their budget in consultation with the Treasury.
- **Main oversight functions** (clause 169(4)) – A number of witnesses in the oral evidence sessions have stated that it would be preferable and simpler for the Investigatory Powers Commission to also oversee the arrangements within Communication Service Providers (CSPs) and public authorities for the retention, storage and destruction of communications data. These matters are currently reviewed by the Information Commissioner's Office (ICO), but in the case of public authorities no audits are undertaken by the ICO. We are responsible for overseeing those arrangements where they concern interception. There are further unhelpful consequences of the overlaps at present between IOCCO's oversight of CSP errors under RIPA and the ICO's oversight of breaches under the Privacy and Electronic

Communications Regulations (PECR) (where the breaches also constitute RIPA errors). In our view there is still considerable room to revise the oversight provisions to simplify the oversight landscape, avoid overlaps and ensure consistency of decision making.

- **Additional Functions Under This Act** (clause 172(2)) – It would be sensible to include an explicit provision for CSPs and staff within public authorities to refer directly to the Investigatory Powers Commission any complaint or concern they have with conduct proposed or undertaken, or any matter on which they require clarification.

b. Full access to technical systems – The current statute (RIPA) contains outdated language (a requirement to provide to the Commissioner with "all such documents and information") and is in need of updating. The query based searches we have developed on the communications data side of our business enable us to identify at scale trends, patterns and compliance issues across large volumes of applications. We need to develop our technical audits on the interception side of the business, particularly where the collection of material and data is at scale.

   Not addressed – The IP Bill must contain provision for the "Commission" to be provided with access to technical systems to assist audits, inspections and inquiries to be carried out. Any new technical systems (e.g. secure automated CSP disclosure systems, the request filter, workflow systems managing applications and authorisations) must be developed with oversight and audit functions in mind.

c. Provision to launch inquires & investigations and sufficient resource to conduct thematic inquiries – The oversight body should have a clear mandate to launch inquiries into matters of public interest or areas of concern. Detailed thematic investigations should take place in addition to ongoing reviews. It is difficult presently for us to produce detailed thematic reports without undermining our core review functions - both are key elements to ensuring robust oversight and one should not compromise the other. Not addressed - Clause 169(1) provides that *"the Investigatory Powers Commissioner must keep under review (including by way of audit, inspection and investigation) the exercise by public authorities of..."* The insertions in brackets appear to be an afterthought and are insufficient. The IP Bill provisions do not compare favourably with the clear powers and legal mandate in place for some of our international counterparts. For example, the oversight provisions for the New Zealand Inspector-General of Intelligence and Security as set out in the Inspector-General of Intelligence and Security Act 1996 (amended in 2013)[471]. The IP Bill oversight clauses could be strengthened significantly in this respect.

[471] See in particular, but not exclusively, sections 11 and 23 - http://www.igis.govt.nz/assets/News/Inspector-General-of-Intelligence-and-Security-Act-1996.pdf

d. Relaxation on secrecy provisions to aid transparency – We are constrained by the current statutory provisions in section 19 of RIPA forbidding disclosure (as are the public authorities and the CSP's). The culture of what appears to be secrecy by default must continue to be challenged and transparency should be encouraged where it leads to greater accountability without prejudicing national security or the ongoing prevention or detection of serious crime.

   Partly addressed – Clauses 43 and 44 provide secrecy provisions for interception-related conduct and create an offence of making unauthorised disclosures (similar to the current section 19 RIPA provisions). The Committee may want to consider whether these provisions are necessary. The provision for "authorised disclosures" in clause 43(5) is however a welcome addition and may lead to greater transparency.

e. Full provision for reporting of errors / breaches and a power to refer to the Investigatory Powers Tribunal (IPT) – It is crucial to ensure that the error reporting provisions are clear and comprehensible and that individuals adversely affected are able to seek effective remedy. On the latter point a number of areas would benefit from review here including; the very high threshold of "wilful or reckless", whether the Commissioner should be able to refer matters or breaches directly to the IPT etc.

   Not addressed - The Bill does not introduce an obvious express power for the Investigatory Powers Commissioner to refer matters to the IPT. We have significant concerns with Clause 171 which, as drafted, confuses and conflates negatively the functions of the Investigatory Powers Commissioner and the IPT. Clause 171 also has significant implications with regard to the ability of individuals to seek effective remedy. Our concerns with Clause 171 are set out in detail in the next section, but a couple of points are worthy of mention here.
   Clause 171 interferes with, dilutes and limits significantly the very well established function of IOCCO to identify and investigate errors and of the Interception Commissioner to make determinations on errors and, where relevant, to inform individuals affected. Clause 171(11) provides that the definition of a "relevant error" will be described in the Codes of Practice. We do not have the draft Codes and therefore it is not possible to assess the detail of this important element.

   We would like to make clear that we are seeking similar provisions for interception errors as we have currently for communications data errors (as set out in Chapter 6 of the current Acquisition and Disclosure of Communications Data Code of Practice). We also felt that it might be pertinent for the Investigatory Powers Commissioner to have the power to refer points of law to the IPT for interpretation where there is perhaps unclear or legally dubious practice. These are two distinct points.

f. Expert resource to complement the Commissioner and inspectors – including technical, legal, privacy advocates, academics etc. Staff in the oversight body should be selected on the basis of expertise and experience. To complement the Commissioners' expertise a wide range of skills is required – former law enforcement and intelligence agency officials, forensic experts, computer scientists, analysts, privacy advocates, lawyers and individuals with media / communications skills. This will ensure that the public authorities are robustly held to account and that all critical views are represented.

   Partly addressed - The oversight impact assessment[472] published at the same time as the IP Bill does set out that technical and other skills will be required within the Investigatory Powers Commission. The budget set out in the impact assessment does represent an increase on the combined budgets for the current three RIPA Commissioners, but until the functions and structure of the Investigatory Powers Commission have been finalised it is impossible to assess whether the budget will be sufficient for the Commission to carry out the oversight effectively.

Clause 171 – Error Reporting

9. Clause 171 is a paradox which requires substantial re-drafting and clarification to ensure that a) the delineation of responsibility between the Investigatory Powers Commissioner and the lPT is clear and, b) individuals are able to seek effective remedy. Our concerns are -

- Clause 171(2) – confuses the role of the Investigatory Powers Commissioner as an audit and investigation body with the role of the IPT as the means by which individuals can seek remedy where they believe they have been a victim of unlawful action under RIPA or human rights infringements in breach of the Human Rights Act 1998. As previously set out this provision dilutes and limits significantly the very well established function of IOCCO to identify and investigate errors and of the Interception Commissioner to make determinations on errors and, where relevant, to inform individuals affected. There is absolutely no need to interfere with that well established power, other than to extend it to interception errors. This cumbersome and unnecessary clause must be removed to ensure effective oversight and achieve greater transparency.
- Clause 171(2) - It seems illogical for the IPT to consider the seriousness of the error and its effect on the person concerned (essentially the merits of the case) before the person has actually brought a complaint to the IPT or the impact of the error has been established.
- Clause 171(2) - there is no definition of "*serious error*" and worryingly the definition appears to be solely dependent on the consequence of the conduct. The assessment of seriousness must have regard to the nature of the conduct itself.

[472] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473777/Impact_Assessment-Oversight.pdf

- Clause 171(3) - the threshold for informing a person of any "*relevant error*" is extremely high. Will the Commissioner or IPT be able to determine if the error has caused *"significant prejudice or harm*" to the person concerned if neither are permitted to contact the person to discuss the matter.
- Clause 171(4) – noting our concerns regarding Clause 171(3) above we also note that the requirement for a serious error is that the breach must be more than simply a breach of a person's convention rights (within the meaning of the Human Rights Act 1998). This threshold does not apply where an individual is seeking to bring an action to the IPT under Section 7 of the Human Rights Act where they merely have to show a public body has or may have acted in contravention of those rights. This is inconsistent and reinforces our concerns that the threshold is being set artificially high. Moreover breaches of Convention rights may be intrinsically serious as in the case of breaches for example of Articles 2, 3 and 5. The fact that there has been an unjustified disclosure of communications data or interception of communications does not of itself justify a finding of a serious error.
- Clause 171(11) – The definition of *"relevant error*" in the IP Bill does not relate to errors by CSPs as it is confined to errors by public authorities. In 2014, 38% of interception errors and 14.3% of communications data errors were attributable to CSPs. Clause 171(7) also only applies to public authorities.

10. No draft Codes of Practice have been published alongside the IP Bill and therefore it is not possible to understand how these provisions will work in practice. There are no error provisions in the current Interception Code of Practice. The error definitions and provisions in the current Acquisition and Disclosure of Communications Data Code of Practice will need to be amended substantially to align to Clause 171 and we have not had the opportunity to review those provisions.

11. Noting the importance of this clause to the entire oversight regime we are of the view that, due to its lack of clarity and the confusion of roles between the Investigatory Powers Commissioner and the IPT, it requires a complete re-draft.

Clause 8 – offence of unlawfully obtaining communications data

12. We have concerns that this new criminal offence will have the unintended consequence of undermining the open and co-operative self-reporting of errors and contraventions of RIPA and the Code of Practice by public authorities. There is a real danger that this provision could reduce accountability because the reporting process depends on individuals reporting to IOCCO at the earliest opportunity when they or their colleagues have made mistakes or when technical systems have failed. The criminal offence may deter some from reporting errors and lead to a subversive error culture. The criminal offence could reduce the shared desire by all parties to work together to resolve errors, prevent recurrence of errors and to strive for continuous improvement. It could perversely result in a greater impact upon an

individual, or impact on a larger number of individuals, than might otherwise have been the case.

13. There is also a real risk that the introduction of this criminal offence will reduce individuals' and public authorities' co-operation with our investigations into any such errors or contraventions. For example, relevant persons whose conduct is questioned may refuse to answer questions or provide information to IOCCO in reliance on the privilege against self-incrimination.

14. There are examples in other legislation where such offences are treated as a collective act by a public authority, rather than an offence by an individual.

Prior authorisation & Post facto oversight

15. There has not so far been much debate as to whether it is desirable for the same body to be responsible for the authorisation of investigatory powers and the post facto oversight of the exercise of those powers. The Committee may wish to consider this point.

16. If it is desirable to have both functions within the same body, then the Judicial Commissioners who are involved in the authorisation of warrants must be operationally distinct from those staff involved in the post facto audit and oversight of the public authorities. Otherwise this could be construed as the Judicial Commissioners "marking their own homework" which would dilute the credibility and independence of the new body. There would of course need to be considerable dialogue between the authorisation and oversight parts of the body to ensure consistency in approach and decision making. It will be crucial to ensure that the oversight section of the body is able to check properly that the information provided to the Judicial Commissioners in the applications was valid and that the subsequent conduct undertaken by the public authority aligned to the authorisation given. It will also be important for the Judicial Commissioners to draw on the technical and operational expertise of the oversight staff. This will provide the Judicial Commissioners with an understanding of the technical and operational aspects of the conduct they are authorising and assist them to consider properly the principles of proportionality and intrusion.

National Security Exceptions

17. There appear to be a number of clauses which provide exceptions for national security or which exempt the intelligence agencies from key safeguards. It would be worth the Committee considering whether those, especially the combined effect, are justified. For example –

- Clauses 47(2) and (3) disapply the requirement for the designated person to be independent from the investigation when approving the acquisition or disclosure of

communications data "in the interests of national security". This dilutes the independence safeguard recently introduced into the March 2015 Communications Data Code of Practice (as a consequence of the *Digital Rights Ireland* case which resulted in a ruling by the ECJ).

- Clauses 60(2) and (3) disapply the requirement for the public authority to consult with a Single Point of Contact (SPoC) when acquiring communications data in the interests of national security. The SPoC is a key safeguard in the process.
- The justification for deeming the interests of national security always to be an exceptional circumstance is unclear.
- Clause 61 is designed to protect the confidentiality of journalistic sources but does not apply to the intelligence services. There is a wealth of case law setting out the importance of protecting the confidentiality of journalistic sources and the very recent judgement by the IPT (in the case of News Group Newspapers Ltd et al vs. the Commissioner of the Metropolis[473]) is also relevant to this matter. Is the exemption of the intelligence services from this provision justified?

Investigatory Powers under Part 2 RIPA and "other" Property Interference under the Intelligence Services Act 1994 or the Police Act 1997

18. The Government has not taken the opportunity to bring all of the investigatory powers used by public authorities into the IP Bill. The result is that there are a number of inconsistencies and a lack of clarity in the authorisation processes in the IP Bill and those in Part 2 of RIPA (e.g. for directed and intrusive surveillance, covert human intelligence sources) and the Intelligence Services Act 1994 and the Police Act 1997 (e.g. interference with "other" property).

19. The IP Bill also curiously prescribes different authorisation and modification procedures for targeted equipment interference warrants made on behalf of the intelligence services or Chief of Defence Intelligence to those made on behalf of law enforcement (see for example clauses 84 and 87 vs. clause 89, clause 96). The different procedures are confusing and it is not clear on what basis they are justified.

Statistical Requirements

20. The IP Bill Committee has asked if we are able to provide some further statistical information relating to interception warrants. In our 2014 Annual Report (published in March 2015) we published the total number of interception warrants issued, the total number extant at the end of 2014, the breakdown of warrants issued by statutory necessity purpose, and the total number of section 8(4) warrants issued. As we set out in our evidence to David Anderson QC's Investigatory Powers Review[474] there are no statistical requirements

[473] http://www.ipt-uk.com/docs/IPT_14_176_H.pdf
[474] http://www.iocco-uk.info/docs/2014-12-5(2)%20IOCCO%20Evidence%20for%20the%20Investigatory%20Powers%20Review.pdf

in the Interception of Communications Code of Practice and the section 19 RIPA secrecy provisions make this area challenging.

21. The Committee has asked specifically if we can provide the number of interception warrants rejected by Secretaries of State. This is not a statistic we have required previously from interception agencies or warrant-granting departments on an annual basis. What we do require the interception agencies and warrant-granting departments to indicate to us during our bi-annual inspections are those warrants which the Senior Official or Secretary of State have either rejected, or those which they have challenged or called for further information before authorising in the period under review (i.e. the previous 6 month period).

22. We have reviewed this information from the first round of interception inspections that took place in 2015 (covering a 6 month period) and have identified that approximately 50 interception warrants were subject to challenge or further information requests by the Senior Official or Secretary of State prior to them being approved. 3 interception warrants were refused in the period covered by those inspections. It is likely that these numbers will cover a mixture of new warrant applications, modifications and renewals.

23. We have previously commented that the rejection figure for interception warrants is inevitably low due to the high level of scrutiny that is applied to each warrant application as it crosses a number of desks in the interception agency and the relevant warrant-granting department before it reaches the Secretary of State. It is important therefore to note that the figure set out in the preceding paragraph does not capture the guardian and gatekeeper / quality assurance function carried out by firstly the staff and lawyers within the interception agency responsible for reviewing all submissions (prior to them being forwarded to the warrant-granting department), or secondly, the guardian and gatekeeper / quality assurance function carried out by staff in the relevant warrant-granting department prior to the warrants' submission to the Secretary of State.

24. The statistical requirements in the Acquisition and Disclosure of Communications Data Code of Practice were enhanced significantly in March 2015, but there are still no statistical requirements in the Interception of Communications Code of Practice. We would welcome the inclusion of statistical requirements into the Interception of Communications Code of Practice to improve transparency and accountability in this area.

Conclusion

25. We would be very happy to provide the Committee with further information on any of the points in this submission, or indeed, on any other elements of the IP Bill.

21 December 2015

Internet Service Providers' Association (ISPA)—written evidence (IPB0137)

1. Summary of key points and recommendations

Full, extensive Parliamentary scrutiny and consultation with all stakeholders

- The Investigatory Powers Bill is a large and highly complex piece of legislation. ISPA is concerned that the Government has set an expedited edited timetable for the consideration of the Draft Bill and has failed to reveal the level of detail that would be required to scrutinise the Bill in depth and properly assess its impact on businesses, customers and citizens both inside and outside of the UK.
- With a more meaningful consultation process that would have involved a wide cross section of the internet community, the Draft Bill could not only have been improved and made easier to understand, but its cost assumptions could also have been put on a robust basis.
- In order to future proof the Draft Investigatory Powers Bill, the Government has built a significant amount of stretch into the Bill – in addition to a more tightly drafted bill, draft of the codes of practices and secondary legislation should be made available at an early stage, ideally, alongside the introduction of the actual Investigatory Powers Bill, to aid Parliament, the public and industry in their scrutiny of the Bill.

Effectiveness on a technical and public policy level

- ISPA has strong concerns that the Bill, as it is currently drafted, does not provide for an effectively tight policy framework and that future governments could change the use of a provision (as stated by the current Government) without further consultation and scrutiny of the impacts on businesses, customers and citizens.
- It will be difficult but possible to implement the provisions of the Bill but this is subject to possibly long time scales and large budgets. It remains for Parliament to determine whether the operational advantages of the data that is being generated justify the public expenditure and interference with the rights of businesses and individuals.
- The interplay between changing definition and existing powers clearly needs to be considered. The Government should explain in more detail what kind of services and providers are likely to covered by the Bill and how they will be affected (particularly in the context of developments such as the Internet of Things). Unless we are provided with further detail on necessity and proportionality, we are also inclined to remove that extension of private networks from the Bill.
- A more detailed and clear explanation of ICRs is necessary before an in depth assessment can be made
- The request filter is a very powerful tool that makes the complex analysis of communications data more easily achievable for public authorities. It remains for Parliament to decide whether these improvements are sufficiently strong to address the concerns raised by the Joint Committee on the Draft Communications Data Bill and to ensure that the Request Filter is used proportionately.
- Provisions on encryption exist in the current law but the Investigatory Powers Bill allows for the application of these powers to new kinds of services and providers that were not envisioned when the current rules were drafted. We urge Parliament to

closely and fully investigate the issue of encryption as there is a real risk that current provision undermines businesses that operate in the UK and the position of the UK as the leading digital economy.

A stable framework that complies with all relevant legal obligations

- It is of fundamental importance that the final Investigatory Power Act complies with all relevant UK and international laws or conventions. A failure to ensure this is likely to result in further successful legal challenges and thus in uncertainty for industry. In cases of legal uncertainty, we urge to err on the side of caution and to not include any provisions in the Bill that have the chance to lead to a successful legal challenge.

Adequate balance of powers, oversight and transparency

- ISPA urges Parliament to undertake a close assessment of whether powers and definitions, e.g. those relating to communications data are drafted appropriately and whether the access requirements and safeguards are appropriate for the level of intrusiveness. Parliament needs to ensure that the level of oversight is scaled up according to the intrusiveness of the powers. The default choice should be to maximise oversight where possible to ensure that users' trust can be maintained.
- Parliament needs to be aware the final Investigatory Powers Act will set an international example that may be followed by less democratic states which may have an impact on UK citizens and businesses.

Full consideration of impact on business

- When assessing the impact of the Bill on businesses it is important to look at the direct, as well as indirect effects, to expand this analysis beyond the UK and to consider monetary as well as non-monetary implications. Only a small set of providers have been consulted and indirect effects, particularly with relation to SMEs may not have been included in the Impact Assessment or full considered.
- The final Act Should enshrine full cost recovery for providers – The cost recovery provision ensures that providers are not commercially disadvantaged and acts as an important safeguard as it provides for a clear link between public expenditure and the exercise of investigatory powers

Conclusion

- A more tightly drafted Bill, updated on a regular basis, with input from stakeholders and parliamentary approval (e.g. via secondary legislation), could be as effective as the current Bill. Such a Bill would, perhaps be less ambitious than the current draft, but it would provide law enforcement and the security services with up-to-date powers, limit the risk of a successful legal challenge and provide parliamentarians, citizens and industry with a better idea of the powers and impacts of the Bill.

About ISPA

1. The Internet Services Providers' Association (ISPA) is the trade association for companies involved in the provision of Internet Services in the UK with around 200 members from across the sector. ISPA represents a diverse set of companies, including those that provide

access to the internet, host websites and data of individuals and business and other cloud-based or over-the-top services.

Introduction

2. ISPA has long been supportive of the creation of a new legal framework to underpin investigatory powers and welcomes that a new draft bill has been put before Parliament for scrutiny. It is widely acknowledged that the existing laws are too complex for legal experts let alone the public or policy-makers to understand, oversight arrangements have not kept pace with the application of the law and various courts and tribunals have found issues with the current arrangements.

3. We start from the position that a limited set of authorities should have reasonable access to investigatory powers to investigate and prosecute crime and safeguard national security. This has to be in compliance with the law, effective, feasible and minimise the impact on business. The Investigatory Powers Bill provides a crucial opportunity to update a hugely complex array of existing surveillance laws.

4. Ahead of publication of the Draft Investigatory Powers Bill we published a checklist of some of the key tests that the Bill needs to pass to ensure an effective outcome. These tests were:
    1. Full, extensive Parliamentary scrutiny and consultation with all stakeholders
    2. Effectiveness on a technical and public policy level
    3. A stable framework that complies with all relevant legal obligations
    4. Adequate balance of powers, oversight and transparency
    5. Full consideration of impact on business

    In the remainder of our response we consider whether these five tests have been met.

Parliamentary scrutiny and consultation with all stakeholders

5. The Investigatory Powers Bill is a large and highly complex piece of legislation. The in-depth scrutiny that is required to do justice to such an important proposal can only be achieved if there is a clear understanding of its scope, aims and implications. This requires the provision of a sufficient amount of time to deliberate the proposals and straightforward and detailed explanations of the aims and powers of the Bill. "Clarity and transparency" was one of the five principles in the David Anderson QC report on investigatory powers and we are concerned that the Government has not only set, yet again, an expedited timetable for the consideration of the Draft Bill, but also has not revealed the level of detail that would be required to scrutinise the Bill in depth.

6. A key recommendation of the Joint Committee on the Draft Communications Data Bill was that further and substantial consultation was needed ahead of new powers being brought

forward. Companies that are currently under a data retention notice (or are likely be to be served with one in the new regime) have been more comprehensively consulted than previously but this deeper level of consultation has not extended to the wider Internet industry. The Bill will not only affect companies that are currently under a data retention notice – some powers can be applied to almost any internet company and, in a fast growing market, some companies may be subject to a notice in the near future. With a more meaningful consultation process that would have involved a wide cross section of the internet community, the Draft Bill could not only have been improved and made easier to understand but it's cost assumptions could also have been put on a robust basis.

Effectiveness on a technical and public policy level

7. The fact that the Draft Investigatory Powers Bill is a highly technical piece of legislation should not be used as an excuse to delink considerations of public policy and technical viability. This needs to be done in two ways:
    1. Can the public policy goals of the Bill be implemented at a technical or administrative level?
    2. Does the Bill set an effective framework to ensure that its provisions do not go beyond the stated public policy goals?

Public policy considerations

8. We set out below that we believe that the Bill can be implemented at a technical and administrative level. However, we have strong concerns that the Bill, as it is currently drafted, does not provide for an effectively tight policy framework. The Government has provided explanations on how it intends to interpret some of the provisions (e.g. in fact sheets, explanatory notes and speeches by Government Ministers) but these explanations are not legally binding and future governments could change the stated use of a provision without further consultation and scrutiny of the impacts on businesses, customers and citizens.

9. In order to future proof the Draft Investigatory Powers Bill, the Government has built a significant amount of stretch into the Bill, resulting in a piece of legislation that is overly broad and whose impact on businesses, citizens and consumer is not fully understood.

10. We are aware that some detail will be provided in secondary legislation, codes of practices and in notices to service providers. We understand that the exact detail of the notices cannot be revealed but we believe that, in addition to a more tightly drafted bill, draft of the codes of practices and secondary legislation should be made available at early stage, ideally, alongside the introduction of the actual Investigatory Powers Bill, to aid Parliament, the public and industry in their scrutiny of the Bill.

Technical considerations

General Technical feasibility

11. Broadly speaking, it should be possible to find technical solutions to implement the provisions of the Bill. However, this is subject to:
    - Time – Service providers will need to develop specific solutions and approaches and the Committee has already heard evidence that the implementation of Internet Connection Records (ICRs) may only be completed in 2018
    - Budgets – The solutions are likely to be highly complex and difficult to implement. The cost estimates that have been provided by the Home Office require further scrutiny and the Committee has already heard that a single provider believes that they will take up the lion's share of the estimated costs.

    When considering the general technical feasibility, it is further worth noting that the technologies that are applied by different providers vary and that different providers thus face different costs. This becomes particularly important if it is decided that smaller providers who have not been consulted so far are included in the data retention regime in the future.

12. Overall, ISPA believes that it will be difficult but possible to implement the provisions of the Bill. However, this may be associated with significant costs and it remains for Parliament to determine whether the operational advantages of the data that is being generated justify the public expenditure and interference with the rights of businesses and individuals. There are also doubts whether the impact assessment fully covers all the possible applications of the provisions in the Bill due to the broadly drafted powers (see below).

Definition of a service provider

13. The Draft Investigatory Powers Bill significantly changes the definition of services providers that are subject to the Bill. This is important as it:
    - Expands the number and types of companies that are subject to and affected by the Bill
    - Changes how existing (and new) powers can be used and implemented, thus effectively creating powers that previously did not exist in the law.

14. Some areas that we would like to point at specifically are:
    - Clause 1 of the Data Retention and Investigatory Powers Act requires a "public telecommunications operator to retain relevant communications data" while the Draft Investigatory Powers Bill only applies to a "public telecommunications operator". This effectively extends the reach of the Bill to private networks, e.g. private company networks or even the communications services within the House of Commons.
    - The definition of a "telecommunications service" is extended in the Investigatory Powers Bill to cover the "provision of access to, and of facilities for making use of, a

telecommunication system include any case where a service consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of such a system", i.e. it may cover actions that are not generally regarded as a communication, e.g. the saving of a document in the cloud.

15. Overall, we are concerned about the unclear and potentially wide-ranging definition of providers and services that are covered by the Bill. The Government has stressed publicly that it has drafted the Bill in consultation with a number of operators that are likely to be served a data retention notice. It is not clear if this has been of a suitably detailed level to enable a full and clear assessment. Moreover, the powers of the Bill could easily be applied to a whole range of other providers and services whose input has not been considered, not least given the new extension to 'private' networks.

16. The interplay between changing definition and existing powers clearly needs to be considered the Government should explain in more detail what kind of services and providers are likely to covered by the Bill and how they will be affected.[475] Unless we are provided with further detail on necessity and proportionality, we are also inclined to remove that extension of private networks from the Bill.

Communications Data definition

17. The Home Secretary has described communications data as "simply the modern equivalent of an itemised phone bill"[476]. We regard this assessment as a mischaracterisation because communications data that relates to modern communications service is far more revealing about an individual's life or behaviour than an itemised phone bill. David Anderson QC came to a similar conclusion in his report on investigatory powers and the Joint Committee on the Draft Communications Data Bill also suggested a "new hierarchy of data types needs to be developed". The Investigatory Powers Bill addresses this through the creation of events and entity data which is a welcome step. However, we would appreciate further information on the Bill's definition that "'data' includes any information which is not data" and urge Parliament to undertake an in-depth assessment of how clearly the definition allow a differentiation between content and communications data

18. Another data type within the Bill is "related communications data" which potentially blurs the lines between intercepted content and communications data. The Bill provides the following definition of related communications data:
    i. "Can be logically extracted from the content of the communication;

[475] Some areas that should be considered in this context are how the Bill will apply to the Internet of Things and machine-to-machine communications and what the privacy impact of this is.
[476] https://www.gov.uk/government/speeches/home-secretary-publication-of-draft-investigatory-powers-bill

ii. Which does not, once extracted, reveal the meaning of the content of the communication; and
iii. Can identify, or assist in identifying, any person, apparatus, telecommunication system or telecommunications service, or which describes an event, or the location of any person, event or thing."

There does not seem to be any clear link between part iii of the definition and the specific communication, i.e. the persons, apparatuses, services or systems could be completely unrelated to the specific communication, e.g. if a database of customers was attached to an email, all the customers' email addresses could be treated as communications data rather than content

19. Overall, we urge Parliament to undertake a close assessment of whether the communications data definitions are drafted appropriately and whether the access requirements and safeguards are appropriate for the level of intrusiveness. The more blurred the lines between content and communications data become, the harder it will be to design and maintain technical equipment to meet this challenge.

Retention and generation of data

20. The Bill goes beyond the current legal framework in that providers will no longer only be required to retain data that is or will be generated for business purposes. Clause 71(8)(b) refers to "collection, generation or otherwise" which suggests that providers may be required to specifically generate data, i.e. it may require providers to change their business operations or make changes to their business model. There have also been suggestion that powers to require the generation of data are similar to third party data retention powers under the Draft Communications Data Bill and we would thus like further information on what exactly is meant by the "generation" of data.

Internet Connections Records

21. An Internet Connection Record is a new concept that has been introduced by the Government alongside the Draft Investigatory Powers Bill. Whilst we understand the challenge of trying to identify who is accessing a communications service, we have three concerns with ICRs:
    1. ICRs are not currently retained or held by service providers for business purposes, i.e. they are an artificial construct that, depending on how the definitions of the Bill are interpreted, will require services providers to produce large volumes of new data sets.
    2. The Investigatory Powers Bill does not provide a clear definition of ICRs making it difficult to assess what data could fall under the definition and what impact the collection of this data may have on businesses and consumers. More details on this

are provided by Graham Smith of Bird&Bird in his written evidence to the Science and Technology Select Committee.

3. The large cost involved in being able to capture and store data associated with ICRs may not be fully met by the figures set out in the Impact Assessment.

22. Overall, this makes an assessment of either the technical or the public policy impact of ICRs very challenging but it is very likely that the retention of ICRs will be technically very difficult and expensive although not impossible. A more detailed and clear explanation of ICRs is necessary before an in-depth assessment can be made.

Request filter

23. Clause 51 provides for a filtering arrangement for communications data. This capability was also proposed in the Draft Communications Data Bill and the Joint Committee that considered this Bill came to the following conclusion:

> *"The Request Filter will speed up complex inquiries and will minimise collateral intrusion. These are important benefits. On the other hand the filter introduces new risks, most obviously the temptation to go on "fishing expeditions". New safeguards should be introduced to minimise these risks. In particular the IoCC should be asked to investigate and report on possible fishing expeditions and to test rigorously the necessity and proportionality of Filter requests"*

24. We largely agree with this assessment. The request filter effectively creates a single distributed database of communications data that is retained in the UK. This database not only allows for simple searches but also complex profiling queries. As such it is a very powerful tool that makes the complex analysis of communications data more easily achievable for public authorities.

25. Accordingly, it will be important to ensure that it the request filter is built in such a way that it provides reliable results, but also that the use of the filter is subject to appropriate proportionality tests. This will need to take into account that the request filter interferes with the rights to privacy of all people whose data is considered as part of a query and not just those people whose data is included in a result. Moreover, there is a need for tight safeguards to ensure that the powerful Communications Data Request Filter is not abused. Compared to the Draft Communications Data Bill, the Draft Investigatory Powers Bill includes a number of improvements, mainly the new Clause 8 offence of knowingly or recklessly obtaining communications data without lawful authority and the creation of a new Investigatory Powers Commissioner. It remains for Parliament to decide whether these improvements are sufficiently strong to address the Joint Committee's concerns and to ensure that the Request Filter is used proportionately.

Encryption

26. Encryption is an essential tool to ensure the security of data and electronic communications. It is widely used by corporations such as banks, is an essential element of the Government's cyber-security strategy and increasingly used by individuals who handle sensitive information or have a general interest in protecting their privacy online. While the Guide to Powers and Safeguards in the Draft Investigatory Powers document states that the "draft Bill will not impose any additional requirements in relation to encryption over and above the existing obligations in RIPA" we urge the Committee to investigate this area in more detail. This is for two reasons:
    1. The provisions relating to encryption may be applied to new kinds of services or providers that were not envisioned when the current rules were drafted
    2. End-to-end encryption is nowadays more common than when the current rules were drafted

27. With this in mind, more information needs to be provided on how the application of Clause 189 (4)(c) would impact providers and services that are widely used by citizens and corporation in the UK. For example, it is unclear how a service provider that offers its customers an end-to-end encryption communications service and thus does not have any access to the encryption keys would be able to comply with a request for the removal of electronic protection. This in turn may also lead to a situation where providers that are based in the UK are commercially disadvantaged compared to their non-UK competitors that are not subject to the same requirements (either because requirements do not apply to them or because they may be unenforceable overseas).

A stable framework that complies with all relevant legal obligations

28. The Committee will be aware that there have been a number of successful legal cases against the use and application of investigatory powers in the UK and EU. The Committee will further be aware of the debate around whether previous court case, particularly the *Digital Rights Ireland* case that was heard in the Court of Justice of the European Union (CJEU), set minimum principles. It has further been pointed out to the Committee that some of the provisions of the Draft Investigatory Powers Bill that have been described as existing powers have never been subject to Parliamentary scrutiny or a full legal assessment, thus putting a question mark on their legal compliance.

29. ISPA is not in a position to provide a clear assessment on these legal matters. However, we believe that it is it is of fundamental importance that the final Investigatory Power Act complies with all relevant UK as and international laws or conventions. A failure to ensure

this is likely to result in further successful legal challenges and thus in uncertainty for industry.

30. If there is uncertainty about the legal compliance of powers in the Bill, especially in light of Court of Appeal referral of the Davis/Watson case to the CJEU[477], we would urge to err on the side of caution and to not include any provisions in the Bill that have the chance to lead to a successful legal challenge.

Adequate balance of powers, oversight and transparency

31. The Draft Investigatory Powers Bill is a highly intrusive piece of legislation and in some areas significantly increases the level of intrusion into the privacy of customers and citizens more widely. The Draft Bill also attempts to strengthen the safeguards and oversight arrangements and we welcome a number of the measures, particularly the creation of an Investigatory Powers Commission. We also note that a limited judicial authorisation regime has been included in the Draft Bill, but are aware that concerns have been raised in relation to its limited application (e.g. exclusion of communications data) and the effectiveness of the double lock system. At present we are not in a position to provide a final assessment in this area but urge Parliament to ensure that the level of oversight is scaled up according to the intrusiveness of the powers. The default choice should be to maximise oversight where possible to ensure that users' trust can be maintained.

Full consideration of impact on business

32. When assessing the impact of the Bill on businesses it is important to look at the direct as well as indirect effects, to expand this analysis beyond the UK and to consider monetary as well as non-monetary implications.
    - A large and potentially expanding number of providers will be directly affected by the Bill, either because they will be served with a notice or a subject to other powers in the Bill.
    - An unknown number of business will be indirectly affected by the Bill and the clearest example is probably that UK providers of security services, hardware and software, but also UK data centres may find it harder to sell in overseas markets due to security concerns of overseas customers.
    - Overseas, non-UK, providers will also be affected as the Government intends to apply some provisions of the Bill extra-territorially which requires some providers to trade-off their own domestic against the UK law.
    - Both UK and overseas businesses may be impacted by other countries following in the footsteps of the UK by adopting similar (but possibly not democratically controlled) investigatory powers regimes, particularly because the UK plays such a leading role in the global digital economy.

[477] https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/11/Davis-FINAL.pdf

33. As explained previously, only a small subset of the providers that will be impacted have been consulted ahead of the application of the Bill and it is not clear whether the indirect effects have been considered by the Impact Assessment. Moreover, it is important to note that the internet, online services and telecommunications are based on a complex interplay of networks and services. Changes within one part of the infrastructure or value chain may have an impact on other parts which usually encourages businesses to share operational information with each other. Some of our members have expressed concern that provisions in the Bill which limit the ability of providers under notice to share information may have unintended consequences.

Costs & Cost recovery

34. The Impact assessment that accompanies the Bill includes an estimated £247m in total and £170.4m in capex costs. This is significantly less than the £859m in the Draft Communications Data Bill. It was made clear during the oral evidence sessions that this figure was arrived at following high level discussions with service providers, and that the true cost of implementing the obligations for a single large ISP would be in the high tens of millions. This is based on the need to procure new hardware to meet new obligations and the high costs of storing large volumes data that would follow. ISPA then expanded on this adding that for some smaller provider the figure could be in the region of £20-30m subject to the exact network requirements. With one single ISP stating in the oral evidence that it would take up the lion's share of the estimated costs, the robustness of the impact assessment is called into question.

35. The Draft Investigatory Powers Bill includes a system for providers to recover their costs. This cost recovery provision is important for two reasons:
    1. It limits the extent to which providers that need to comply with the relevant provisions are commercial disadvantaged.
    2. It acts as an important safeguard as it provides for a clear link between public expenditure and the exercise of investigatory powers and this provides an effective way for ensuring that powers are used where necessary.

36. At present, the Draft Bill only guarantees that the contribution of the Government to a provider's costs cannot be zero but we believe that, for the two stated reasons, it is important to enshrine full cost recovery on the face of the Bill. The current draft would enable future Government to scale back their contribution to costs and thus not only put providers at a commercial disadvantage but also risk undermining an important safeguard.

Conclusion

1. The Draft Investigatory Powers Bill is an extremely complex and wide-ranging piece of legislation and the information that has been provided so far makes it difficult to scrutinise the Bill in-depth. However, it is clear that the Bill will have a significant impact on providers, customers and citizens, both inside and outside of the UK. We are concerned that some of the provisions in the Bill are too wide-ranging and that the impact of these powers, particularly in the context of fast a changing communications and technology environment (e.g. the rollout of the Internet of Things), is not fully understood.

2. Industry fully supports the creation of a new legal framework for investigatory powers. This new Bill needs to be fully compliant with the law, be effective, feasible and minimise the impact on business and customers. We believe that a more tightly drafted Bill, updated on a regular basis, with input from stakeholders and parliamentary approval (e.g. via secondary legislation), could be as effective as the current Bill. Such a Bill would, perhaps be less ambitious than the current draft, but it would provide law enforcement and the security services with up-to-date powers, limit the risk of a successful legal challenge and provide parliamentarians, citizens and industry with a better idea of the powers and impacts of the Bill. This could further be combined with an appeals process for providers that are served with a retention notice, that is independently judged rather than stopping with the Secretary of State.

Internet Service Providers' Association (ISPA)—supplementary written evidence (IPB0164)

Introduction

1. This supplementary evidence from the Internet Services Providers' Association follows publication of the Home Office's response to Joint Committee and sets out additional information on Internet Connection Records (ICR).

2. In our written and oral evidence, we explained that the term ICR is not used by industry and the lack of detail provided made it difficult to fully analyse its impact. We further explained that to get the necessary data to help identify a communication or device to a service – the intention of an ICR - would require the retention of very large volumes of data that it is not currently retained or fully costed for.

3. In her oral evidence to the Joint Committee on 13 January 2016, the Home Secretary suggested that she did not recognise the degree of uncertainty surrounding ICRs and that ISPs were "reassured". To be clear, we still view the term ICR as imprecise and requiring further work. We set out our reasoning for this below.

Internet Connection Records

4. We welcome the fact that the Home Office has provided some additional detail on ICRs to the Committee. However, we should have seen a more detailed level of explanation when the Bill was published as the term remains imprecise, not least as this was trailed as the only new significant increase in capabilities. As explained, ICR is not a recognised term, and its broad wording has the potential to include vast amounts of data that our members do not retain, and potentially cannot retain, for business purposes. In order to meet the obligations or attributing IP addresses to users, services or a device, it could involve some communications services having to be altered or redesigned. That the draft Bill only references ICRs in two clauses (47 on restrictions and 71 on retention powers) has added to the sense of uncertainty.

5. In its supplementary evidence, the Home Office sets out a number of components that an ICR may be composed of, including core parts. It is remains unclear if additional components could also be included within an ICR and if so what and how these would be added. The example ICR given is only one scenario, there are bound to be other potentially more complex uses. We would welcome a fuller explanation of new data types that could be included under an ICR.

6. The Home Office evidence says that it will not require providers to retain certain data (URI domain or service identifier) if this constitutes third party data and is not processed for business purposes. These assurances should be made clear in the legislation. In introducing the legislation, the Home Office stressed that third party data retention powers were not included in the draft Bill having dropped the proposals from the Draft Communications Data Bill. We recommend that the Bill prohibits any retention or generation of third party data not processed for business purposes; the restrictions in Clause 47 should make this clear.

7. We surmise from the further evidence provided that the Home Office wants full TCP level session stats to be logged, including Network Address Translation (NAT) sessions. Not all ISPs

retain this data or have the necessary hardware to capture and retain this. If an ISP has a NAT device it may be viable, even then it would involve a large volume of data and a number of significant challenges would have to be worked through. As was highlighted by large consumer providers in their oral evidence, the figure of £174m in the impact assessment is not likely to be sufficient to cover the increase in retained data retained. Meeting the demands of the Home Office as set out may be viable for some providers, but the costs at this stage appear to be underestimated and there are significant technical and operational challenges for each provider.

8. The Home Office says that TCP Multipath flag may be required in the future. We assume this is to related to multicast traffic. Under what circumstances would the TCP Multipath flag be required?

9. ICRs also include access to web browsing activity up to the first slash. Evidence has been submitted from a privacy and proportionality perspective but it also needs to be looked at from a technical perspective. Websites may consist of a wide variety of content drawn from an array of sources – social media feeds, plug-ins, adverts, etc. Would CSPs be expected to capture all this data to help determine when a user or device has connected to a communication service?

10. When assessing the privacy impacts of ICRs, we urge the Committee to also include the impact of the request filter. It can be reasonably argued that the combination of ICRs with the request filter creates new insight that is potentially far more revealing than anything that is currently available to law enforcement. In the current regime, access to that level of similar data can only be obtained through equipment interference, which is governed by a higher authorisation threshold. It is for this reason that access and oversight needs to be stepped up in line with the privacy implications.

Conclusion

11. In summary, in relation to ICRs we are calling for the draft Bill to:

- Provide a full explanation of new data types that could be included under an ICR
- Prohibit any retention or generation of third party data not processed for business purposes
- Review the costs of implementing the proposals
- Review the oversight arrangements for ICRs

12. Whilst the additional information from the Home Office has shed some further light on what types of data may be included in an ICR, further information is required to help adequately analyse the proposals. The Bill's scrutiny is progressing at a fast pace, and there are still a number of unanswered questions about what constitutes an ICR and the practicalities in actually accessing and retaining this data. Until then it remains difficult to give a definitive analysis on ICRs.

18 January 2016

IT-Political Association of Denmark—written evidence (IPB0103)

Introduction

1. IT-Political Association of Denmark (IT-Pol) is a Danish civil society organisation that works to promote privacy and freedom in the information society.[478] The activities of IT-Pol are funded entirely by membership contributions. IT-Pol is regularly consulted by Danish news media and politicians about the technical and privacy aspects of data retention.

2. This submission contains comments on the proposal for internet connection records (ICRs) in the draft Investigatory Powers Bill.[479] The motivation for ICRs in the Draft Bill and the outlined retention requirements are very similar to the session logging data retention scheme which was used in Denmark from 2007 until 2014 when it was repealed for lack of effectiveness.

3. For proper context, our written evidence will start with a description of session logging and a summary of the self-evaluation report published by the Danish Ministry of Justice in December 2012. This will be followed by our comments on the proposed ICR scheme and recommendations for the British Parliament. These remarks are based on our ongoing analysis of session logging in Denmark, adapted to our reading of the ICR proposal in the draft Investigatory Powers Bill.

Session logging in Denmark

4. Danish data retention took effect in September 2007 with ”logningsbekendtgørelsen”[480], and consisted of two parts: the data retention requirements for telephony and internet access in the now annulled European Data Retention Directive (2006/24/EC) and the special session logging requirements for internet traffic, described in paragraphs 5-6.

5. Under session logging, the following information about internet packets must be retained: source and destination internet protocol (IP) address, source and destination port number, transmission protocol (like TCP and UDP), and timestamp.[481]

6. The main rule was to retain this information for the first and last packet of an internet session, which is not precisely defined. Alternatively, an internet service provider (ISP) could retain information about every 500th packet (known as “sampling”) at the boundary of their network where traffic is exchanged with other

478 Website of IT-Pol Denmark: https://itpol.dk/

479 Some of the material in this written evidence was submitted to the Science and Technology Committee earlier http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25190.html

480 Logningsbekendtgørelsen (Danish administrative order for data retention). The original order is available at https://www.retsinformation.dk/forms/r0710.aspx?id=2445. An English translation done by the Ministry of Justice is available at https://itpol.dk/sites/itpol.dk/files/TFR40200.pdf

481 Section 5(1) in the administrative order https://itpol.dk/sites/itpol.dk/files/TFR40200.pdf

ISPs. This rule was used by most ISPs in practice.

7. The purpose of session logging was to retain information about all types of internet communication between two individuals, similar to data retention for telephony. The intention by the Ministry of Justice was that the destination IP address and port number could identify the particular communication service being used.

8. The specific retention requirements in paragraphs 5-6 reflect a compromise negotiated between the Ministry of Justice and the Danish ISP industry. For large ISPs, it was important that the information could be collected at the boundary of their network as this reduced the investment in the technical equipment needed for session logging. Moreover, by limiting the retention requirements to IP addresses, and not server (domain) names, the task could be performed without Deep Packet Inspection (DPI).

9. In December 2012, the Ministry of Justice published a self-evaluation report about Danish data retention.[482] According to the report, communication data from session logging had only been used in a limited number of cases. The only example given in the self-evaluation report was a case involving online banking fraud on a minor scale. The Danish Security and Intelligence Service (PET), which is responsible for domestic counter-terrorism in Denmark, stated in the report that it had only been relevant to request session logging information in a very limited number of investigations by the service.

10. The report mentioned technical difficulties by the Danish police in handling the massive amount of data available through session logging. In 2013, about 3500 billion records about telecommunication were retained in Denmark (620000 per citizen), of which more than 90 percent was due to session logging.

11. The report also highlighted a limitation of collecting session logging information at the boundary of the ISP network. When multiple customers share the same public IP address with Carrier-Grade Network Address Translation (CG-NAT), commonly used for internet access on mobile phones, the individual customers could not always be separately identified. This was a negative consequence, probably unforeseen, of a technical compromise which sought to reduce the cost of session logging for the ISPs.

12. On 2 June 2014, the Danish government decided to repeal session logging.[483] The Ministry of Justice emphasised that session logging was repealed solely because it had been unable to achieve the stated objective (investigation and prosecution of crime). Therefore, the Ministry of Justice did not include session logging in its legal

482 The data retention self-evaluation report from the Ministry of Justice is available at http://www.ft.dk/samling/20121/almdel/reu/bilag/125/1200765.pdf. There is no English translation. The article "In Denmark, Online Tracking of Citizens is an Unwieldy Failure" in TechPresident, 22 May 2013, covers the report. Available at http://techpresident.com/news/wegov/23918/denmark-government-will-not-allow-ordinary-citizens-have-digital-privacy

483 Press release: The Ministry of Justice repeals the rules about session logging, 2 June 2014 http://www.justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2014/justitsministeren-oph%C3%A6ver-reglerne-om-sessionslogning (in Danish)

analysis of the data retention judgment from the Court of Justice of the European Union (CJEU), which was published on the same date.[484]

13. The Ministry of Justice has indicated that session logging could be re-introduced if the technical problems can be properly addressed, and the Ministry of Justice would discuss this issue with the Danish ISP industry. To date, no proposal for a revised session logging scheme has been put forward.

Definition of Internet Connection Records in the Investigatory Powers Bill

14. It is natural to compare ICRs to call detail records (CDRs) from telephony which contain information about the calling party (A-number), called party (B-number), starting time and the duration of the call. CDRs are collected because they are needed to billing in most cases.

15. ICRs on the other hand do not naturally exist in the technical infrastructure of an ISP. The information contained in ICRs is used by the ISP for routing internet traffic, but the information is not regularly retained because it is not needed for billing. Customers may pay for data volumes, but almost never based on the destination of the internet traffic. This implies that ICRs will have to be created by the ISP in order to be retained.

16. Second, and more importantly, it is inherently difficult to define ICRs in a meaningful way. Unlike the telephone system, the Internet Protocol is stateless. A telephone call has a certain duration, which the telecommunication company can keep track of because a telephone line is in use. Internet traffic is divided into packets which can be routed independently of each other between the end-points (source and destination IP addresses), and only the end-points can associate the individual internet packets with a particular mode of communication.

17. Retaining information about every internet packet, or even every 500th packet as in the Danish session logging scheme, will generate a lot of data. The maximum size of an internet packet is 1500 bytes, so something as simple as a reading an article from an online newspaper will typically generate thousands of internet packets, not just to the web server for the newspaper itself, but also to the many third-party elements that are often included on web pages, for example social-media elements and online advertising.

18. The destination address in an ICR could be an IP address, as in the Danish session logging scheme, or a domain (server) name. The wording in Clause 71(9)(f) of the draft Investigatory Powers Bill covers both possibilities. When the internet communication takes place, a domain name (such as www.parliament.uk) is translated to an IP address through a DNS lookup and the IP address is used for routing the traffic, but the DNS information is generally not available to the ISP in a

484 A summary of the legal analysis of the CJEU judgment by the Danish Ministry of Justice can be found in the EDRi-gram article “Denmark: Data retention is here to stay despite the CJEU ruling", 4 June 2014, available at: https://edri.org/denmark-data-retention-stay-despite-cjeu-ruling/

form whereby it can be readily associated with the ICR. Instead, some form of DPI will be required if ICRs include server names, and this will substantially increase the cost of data retention. With the increasing use of encryption for web traffic (HTTPS), it may even be impossible to determine the server name with DPI.

19. Instead of including the server name in the ICR definition at the time of collection, the police could attempt to associate the destination IP addresses with server names when the ICR information is obtained by the police in specific investigations. This avoids the potentially costly use of DPI by the ISP, but there are also disadvantages. Multiple websites are often hosted on the same server with the same IP address, which means that the server name cannot be uniquely determined from the IP address. Furthermore, IP addresses of some servers change over time, so the DNS information may have changed between the time of the actual communication and the police investigation, which could be up to 12 months later.

20. ISPs will have to invest in special equipment in order to be able to retain ICR information about their customers since this is not a regular task for an ISP. Depending on how ICRs are defined, it could even be the case that ISPs would have to make changes to their technical infrastructure in order to satisfy specific ICR retention requirements. This is something that all British ISPs must prepare for, even if they have not yet been served with an ICR retention notice by the Secretary of State.

Privacy implications of ICR data retention

21. Collection of ICR information will be extremely intrusive to the private lives of British citizens. The destination IP addresses will, in some cases, contain sensitive information about political and religious preferences of citizens through their choices of online news media, visits to websites of political parties and candidates as well as religious groups and societies. The health conditions of citizens could be revealed through the frequency of visits to websites with information about specific diseases and medical conditions, even when the individual web pages (URLs) are not retained.

22. ICR data retention could also have negative implications for the freedom of information of British citizens if they refrain from visiting certain websites out of fear that their visits to these websites will be registered by their ISP. A recent study by PEN International shows that a high number of writers in democratic societies have refrained from conducting internet searches or visiting websites due to fear of government surveillance.[485]

Device identification

23. One of the objectives of ICRs in the draft Investigatory Powers Bill is to identify the individual device that has sent a communication online.[486] A typical case scenario is

485 "Global Chilling: The Impact of Mass Surveillance on International Writers", PEN International, 5 January 2015. Available at: http://www.pen.org/sites/default/files/globalchilling_2015.pdf

486 Purpose 1 on page 14-16 of "Operational Case for the Retention of Internet Connection Records", part of the

that the police obtains an IP address during an investigation and asks the ISP for the name of the customer that has used this IP address. If public IP addresses are shared with CG-NAT, the same IP address could be assigned to a thousand customers at any given time. If ICRs are available, the ISP will then be asked to search for the customers who had traffic to the specific destination IP address at the time (using the "request filter" proposed in the Draft Bill), and this will reduce the number of customers on the list, ideally to a single customer, but this is not guaranteed.

24. This application of ICRs is highly dependent on accurate timestamps on both ends, that is the ICR data retained by the ISP and the timestamp associated with the IP address that the police has discovered during its investigation. The accuracy of the latter timestamp will often be hard to verify for the police. If timestamps are not accurate, the wrong person might be identified from this application of the request filter.

25. Furthermore, there are limits as to what devices an ISP can actually identify. In general, the ISP can only identify devices that are connected directly to the ISP. A smartphone can be identified when it uses mobile data for its internet connection as this involves a direct connection between the smartphone and the ISP. However, if the smartphone connects to the internet through a WiFi access point (for example a WiFi hotspot in a hotel or pub), the ISP serving that access point only sees connections coming from the access point device itself. This means that the ISP is unable to distinguish between the individual devices (for example smartphones and laptops) that may be connected to the internet through the access point.

Further limitations of using ICRs in police investigations

26. The ICR data for an individual will contain a complete profile of the behaviour on the internet of that individual, subject to the limitation mentioned in paragraph 27 below. This includes all communication services accessed, at least to the extent that they can be determined from the destination IP addresses. However, the number of records in this data set will be really large. Many individuals use file sharing software or online gaming that tend to generate lots of internet packets to unknown IP addresses. Activities as simple as web browsing generate requests to numerous third-party websites for online advertising, social media elements and user tracking. Looking for traffic to illegal websites or communication services could be a "needle in the haystack" problem. In Denmark, this has been a practical problem for the police when analysing data from session logging.

27. It is very easy for an individual to hide the final destination of the internet traffic and make the ICR data useless from the viewpoint of law enforcement. If the individual uses a VPN connection, the destination address in the ICR will be that of the VPN server, not the real destination of the traffic. Even if VPN providers are subjected to similar ICR retention requirements, it will only apply to UK VPN providers and not foreign ones. Another possibility is to use Tor (a well-known anonymisation network), in which case the ICR will contain information about random Tor entry nodes, not the

overarching documents for the draft Investigatory Powers Bill.

final destination of the traffic. It is very likely that the use of VPN and Tor will increase when the public becomes aware of ICR data retention.

Economic considerations

28. In addition to the collection of ICRs from internet packets, ISPs must also make the retained data available to law enforcement through the "request filter" system in clauses 51-53 of the Draft Bill.

29. The factsheet for the request filter says that "public authorities will sometimes need to make complex queries". This suggests that the entire collection of ICRs would need to be searchable through the request filter, which means that ISPs would have to build a potentially very large and scalable database infrastructure in order to support the requirements under the request filter. The cost of building and maintaining this database system could be quite substantial. Since the request filter involves external access to the database by design, there are also security considerations and security costs associated with preventing unauthorised access to the system.

30. Since these systems are not necessarily trivial to implement, ISPs may have to acquire these systems before they are served with a retention notice for ICRs. This of course depends on the deadline given in a retention notice. These costs, if not fully covered by the British Government, are likely to have a substantial fixed element which would effectively discriminate against smaller ISPs and new companies that consider entering the ISP business. That would have negative consequences for the competition landscape and consumer choice for internet access services.

Recommendations for the British Parliament

31. First of all, IT-Pol would encourage the British Parliament to carefully consider whether data retention with ICR is really a feasible project. In paragraphs 14-30, we have pointed out that ICR data retention invariably will involve a number of technical compromises that could either lead to very high costs or severe limitations in the use of ICRs. The Danish experience with session logging, as documented in the first part of this written evidence, has been strongly negative.

32. If ICR data retention is adopted, the specific retention requirements should be negotiated with the ISP industry. The ISPs have the technical expertise as to what is technically feasible, and only the ISPs can make realistic projections about the costs. These costs will be highly dependent on how the networks are currently structured.

33. Even if it is possible to build an ideal ICR retention system, from the viewpoint of law enforcement, which is likely to be very expensive, it will be really trivial and cheap for individuals to circumvent this type of data retention by using VPN connections or the Tor network.

21 December 2015

Jisc—written evidence (IPB0019)

1. Jisc is the UK's expert body for digital technology and digital resources in higher education, further education and research. Since its foundation in the early 1990s, Jisc has played a pivotal role in the adoption of information technology by UK universities and colleges, supporting them to improve learning, teaching, the student experience and institutional efficiency, as well as enabling more powerful research.

2. In particular Jisc is the operator of Janet, the UK's world-leading National Research and Education Network (NREN), connecting around a thousand universities, colleges and research organisations to each other, to peer NRENs around the world, and to the global Internet.

3. Janet, and the networks of the organisations it connects, are classed as a private electronic communications services or networks under current telecoms and security legislation. We have been working satisfactorily within the *Regulation of Investigatory Powers Act*'s regime for communications data disclosure since 2000, but have not previously been subject to data retention requirements.

4. Our response is therefore concerned with the new powers and greatly increased scope of the draft Bill.

Are the powers sought workable and carefully defined?

5. The draft Bill contains two extensive new powers for the Home Secretary, to enter into "filtering arrangements" (clause 51) and "technical capabilities" (clause 189). These require telecommunications operators to modify their systems in ways that will facilitate the future exercise of powers to obtain, respectively, communications data and content. However, unlike previous legislation in these areas, the Bill contains no statutory limit on the types of modification that may be required. Previous legislation has limited such measures to specific types of communications data (e.g. "relevant communications data" in s.2(1) *Data Retention and Investigatory Powers Act 2014*) and to data "generated or processed" by the recipient of the order (s.2(1) *DRIPA*). The only limitation on the face of this draft Bill is that a requirement be technically feasible (c.190(3)(c)). In responding to the enquiry's question, we conclude that these powers are not, in fact, defined.

6. Furthermore the range of organisations to which these powers apply has been greatly increased. Under current law, orders to prepare for future investigations (for example by data retention or interception capabilities) can only be made against "public telecommunications operators" (see *DRIPA* s.1(1) and *RIPA* s.12(1)(a)). Private networks – such as Janet and networks within universities, colleges and businesses – can be required to disclose specific communications data they already have (*RIPA* s.22) or to implement targeted interception warrants (*RIPA* s.5). However they cannot be required to modify their activities or systems in advance so as to facilitate such activities. The new Bill applies all its powers, both preparatory and targeted, to "telecommunications operators": a term defined in clause 193 so as to include every organisation and home with any kind of connection to a telecommunications network.

Are the powers necessary? Has the case been made…?

7. These expansions in both the scope of powers and the range of organisations covered are not mentioned in the explanatory notes to the draft Bill, the cost estimates, or (so far as we are aware) the Home Office's oral evidence to the Committee. The only new power mentioned is adding "Internet Connection Records" (c.47(6)) to the types of communications data that public networks may currently be required to retain. We therefore conclude that the Home Office has not made the case for the much greater expansion of powers and scope that the draft Bill text contains.

8. While we have no information to enable us to comment on the benefits that these additional powers might bring, we do foresee the potential for considerable harm to users of communication systems in the UK, both individuals and organisations.

9. Preparatory measures, whether "filtering arrangements" or "technical capabilities" will inevitably affect all communications through the systems to which they are applied, not just those that are the focus of subsequent warrants. In many cases they will increase the risk to all users: retaining extra communications data will increase the impact of security breaches as well as creating a more attractive target for fraudsters and other hackers; systems to facilitate law enforcement access to communications may be discovered and exploited by criminals, as lawful intercept systems on mobile phone networks and master keys for luggage have been in the past.

10. Even if these powers are not used, their existence and increased scope will reduce trust in all "telecommunications operators" (i.e. all UK organisations) as safe places to store or process data. Since it will be a criminal offence to reveal that an organisation is providing either "filtering arrangements" or "technical capabilities", organisations will have no way to counter suspicions that they are doing so. Other countries' Information Technology sectors have already experienced the loss of international business that results from such suspicions. This could be particularly harmful for universities, colleges and research centres whose national and international research partners – for example in the high-tech or healthcare sectors – have high expectations that shared data will be kept confidential.

11. Even if these harms are justified by the need for communications data or interception, we consider that some actions falling within the definitions of "filtering arrangements" and "technical capabilities" would be so damaging to security and trust in the UK internet that the Bill should explicitly prohibit them. The draft Bill would, for example, allow the Government to order weaknesses to be introduced that reduce the integrity of networks, online applications or cryptographic systems. Each of these would, however, satisfy the draft Bill's tests of being technically feasible and facilitating access to communications data or content. If a threat ever becomes so high as to require a reduction in the security of systems that UK citizens and businesses rely on, we consider that this should be debated and approved by Parliament using specific primary legislation.

15 December 2015

Rt Hon. Lord Judge—supplementary written evidence (IPB0020)

May I add a word about the system for appointments.

In the discussion on page 28 my observations were being directed to the process of the appointment of Commissioners in the context of those who are no longer serving judges. For judges currently in office the only viable system is for the Lord Chief Justice to assign them to work as Commissioners. As a matter of principle judicial deployment is acknowledged to be a crucial responsibility of the Lord Chief, who not only has the clearest understanding of the experience and skills of all the judges, but who also knows those judges who will be serious candidates for the Court of Appeal where new experiences as commissioners would be valuable. No less important, he will have to address the consequences of the drain on judicial resources in the High Court and Court of Appeal of seconding senior judges to the Commission.

I am perfectly happy to give further evidence if required, and understand that this letter will be treated as a public document.

15 December 2015

Justice—written evidence (IPB0148)

Summary

In 2011, JUSTICE recommended that the Regulation of Investigatory Powers Act 2000 ('RIPA') be repealed and replaced by a modern legal framework for surveillance more suited to a digital age. Reconciling the right to respect for privacy and the security interests of the wider community requires careful consideration, but the public interests in privacy and security are not mutually exclusive. Surveillance is a necessary activity in the fight against serious crime. When targeted, it can play a vital part in our national security.

Building a legal framework for surveillance in the digital age is now a priority. However, JUSTICE is concerned that the Draft Bill, like the Draft Communications Data Bill before it, includes broad provision for untargeted and bulk powers of surveillance. We raise concerns about the compatibility of these powers with the provisions of the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union. While others will be better placed to advise the Committee on the practical impact of these powers or the operational case to support them, JUSTICE urges the Joint Committee to subject the Government's legal analysis to close scrutiny before a Bill is presented to Parliament.

JUSTICE focuses on a number of specific issues in our submission:

(i) The Draft Bill should be amended to provide for judicial authorisation of warrants as a default, subject to a limited exception for certification by the Secretary of State in some cases involving defence and foreign policy matters.
(ii) Any provision for judicial authorisation should provide that the Judicial Commissioner is able to conduct a full merits review of the necessity and proportionality of an individual measure.
(iii) The urgent procedure in the Bill should be amended to restrict the capacity for its arbitrary application.
(iv) Any modification of warrants should be made by a Judicial Commissioner.
(v) Judicial Commissioners considering applications should have access to security vetted Special Advocates to help represent the interests of the subject and the wider public interest in protecting privacy.
(vi) The resources for the new Investigatory Powers Commission ('IPC') should not be managed by the Secretary of State (who may be subject to its scrutiny).
(vii) Any drain on the High Court when judges take up appointments as Judicial Commissioners should be offset by the Treasury.
(viii) The independence of the Commission will be paramount to its effectiveness.
(ix) The judicial functions of the Judicial Commissioners and the wider investigatory and audit functions of the Commission should remain operationally distinct. While it would, in our view, be beneficial for the Commissioners to be able to draw upon the wider expertise provided by the staff of the Commission, there should be no doubt about their capacity to take independent decisions on individual warrants.
(x) Judicial Commissioners should be appointed by the Judicial Appointments Commission not the Prime Minister.

(xi) The Draft Bill should be amended to put beyond doubt that the Commission can conduct own-initiative inquiries.
(xii) Clause 171 on reporting of errors should be substantially amended. At a minimum, it should be accompanied by a mandatory disclosure requirement for individuals targeted for surveillance to be provided with information after-the-event.
(xiii) The Draft Bill should be amended to create a safe-route to the IPC, making clear that communications from officials or Communications Service Providers will not be treated as a criminal offence for any purpose.
(xiv) The new right of appeal from decisions of the Investigatory Powers Tribunal is welcome. The Draft Bill should be amended to clarify that a right of appeal lies from all rulings of the Tribunal, not only final determinations. The route of appeal should be clear on the face of the Bill, not left to be determined in secondary legislation by the Secretary of State.
(xv) JUSTICE considers that the Draft Bill should be amended to modernise the procedures of the IPT. This should include an amendment to provide for the IPT to be able to make declarations of incompatibility pursuant to Section 4, Human Rights Act 1998.
(xvi) The Draft Bill should be amended to provide greater protection for legal professional privilege and for the communications of politicians and journalists.
(xvii) The ban on the use of intercepted material in criminal proceedings, in Clause 42, should be removed.

(a) Introduction

1. Founded in 1957, JUSTICE is a UK-based human rights and law reform organisation. Its mission is to advance access to justice, human rights and the rule of law. It is also the British section of the International Commission of Jurists. In 2011, we published *Freedom from Suspicion: Surveillance Reform for a Digital Age,* calling for the wholesale reform of the existing legal framework for surveillance.[487] In anticipation of the publication of the Draft Investigatory Powers Bill for consultation, we published an update to that report, *Freedom from Suspicion: Building a Surveillance Framework for a Digital Age.*[488]

2. We welcome the opportunity to submit written evidence to the Joint Committee on the Draft Investigatory Powers Bill ('the Committee'). We regret the short time available for consideration of the Draft Bill by the Committee and by the wider community. The Draft Investigatory Powers Bill ('the Draft Bill') was published on 4 November and the Joint Committee is required to report by 11 February. In practice, the Joint Committee will conclude its work in around 7 weeks. We are concerned that, to provide scrutiny of a technically and legally complex Bill of almost 300 pages, this timescale is very short and will limit the effectiveness of pre-legislative scrutiny by Parliament, commentators and the wider public.

---

[487] JUSTICE, *Freedom from Suspicion: Surveillance Reform for a Digital Age,* Nov 2011. Hard copies of this report have been provided to members of the Joint Committee. http://www.justice.org.uk/resources.php/305/freedom-from-suspicion Hererin, '*Freedom from Suspicion*'.
[488] JUSTICE, *Freedom from Suspicion: Building a Surveillance Framework for a Digital Age,* Nov 2015. . Hard copies of this report have been provided to members of the Joint Committee. http://2bquk8cdew6192tsu41lay8t.wpengine.netdna-cdn.com/wp-content/uploads/2015/11/JUSTICE-Building-a-Surveillance-Framework-for-a-Digital-Age.pdf Hererin, '*Freedom from Suspicion: Second Report'.*

3. In this submission, JUSTICE focuses principally on issues of authorisation and the judiciary; oversight and the role of the new Investigatory Powers Commission ('IPC') and the Investigatory Powers Tribunal ('IPT'). We raise some wider concerns about the treatment of privileges, legal professional privilege, in particular, and the treatment of intercept material as evidence in legal proceedings. Given the short time available, we focus on the issues most closely allied to our current work and expertise.

4. Where we do not specifically address an issue, or question posed by the Committee, this should not be taken as support for the proposals in the Draft Bill.

(b) Background

5. The Draft Bill fulfils a commitment by Government to produce new legislation to replace the Data Retention and Investigatory Powers Act 2014 in draft for consideration by a pre-legislative committee of both Houses. Part 1 provides for a number of offences which relate to the misuse of powers relating to surveillance. Part 2 deals with the interception of communications by security agencies, law enforcement bodies and others. Parts 3 and 4 deal with the retention of communications data and access to that material. These parts replace the Data Retention and Investigatory Powers Act 2014 ('DRIPA'). They expressly empowers the Secretary of State to request the retention of 'Internet Connection Records'. Part 5 governs "Equipment Interference" (also known as hacking or Computer Network Exploitation). Part 6 creates a framework for 'bulk interception' warrants and for bulk warrants for the acquisition of communications data and equipment interference. Part 7 provides for access to bulk personal datasets. Part 8 provides for the creation of a new single oversight body, the Investigatory Powers Commission ('IPC') and proposes a new right of appeal from decisions of the Investigatory Powers Tribunal ('IPT').

6. Since 2011, JUSTICE has recommended that the Regulation of Investigatory Powers Act 2000 ('RIPA') is repealed and replaced by a modern legal framework for surveillance. Reconciling the right to respect for privacy and the security interests of the wider community requires careful consideration, but the public interests in privacy and security are not mutually exclusive. Surveillance is a necessary activity in the fight against serious crime. When targeted, it can play a vital part in our national security.

7. Building a legal framework for surveillance in the digital age is now a priority. In the past year alone, the IPT has found violations of the right to privacy under Article 8 of the European Convention on Human Rights ('ECHR') by the intelligence services on three different occasions, the Divisional Court has disapplied section 1 of DRIPA because it breached the rights to privacy and data protection under the EU Charter of Fundamental Rights,[489] and the Intelligence and Security Committee and the Independent Reviewer of

[489] *Davis, Watson & Ors v Secretary of State for the Home Department and Ors* [2015] EWHC 2092 (Admin). This decision is subject to appeal and the Court of Appeal has referred a number of the questions to the Court of Justice of the European Union. See [2015] EWCA (Civ) 1185.

Terrorism Legislation have each produced major critical reports on the legal framework governing surveillance powers.[490]

8. While the powers sought in the Draft Bill are more readily comprehensible than in the previous, much criticised, Draft Communications Data Bill,[491] many of its provisions provide for the use of untargeted and bulk powers of surveillance:

   a. **Comprehensive and comprehensible?** We welcome the decision in the Draft Bill to move away from the legislative model adopted in the Draft Communications Data Bill, which created broad powers for public bodies and duties for Communications Service Providers ('CSPs') and left details and safeguards to secondary legislation. We welcome the Government's decision to accept the recommendation of the Anderson Review that powers should be avowed in so far as possible. While in practice this approach increases the size of the Bill, we welcome the efforts made by Government to increase clarity in the powers sought.

      The Bill contains 202 clauses and 8 separate Schedules. While lengthy it doesn't replace the Regulation of Investigatory Powers Bill 2000 ("RIPA") in its entirety. The Bill deals with communications surveillance and replaces Parts 1 and 4 of RIPA, together with powers in other pieces of legislation. Other forms of surveillance – including the use of Covert Human Intelligence Sources – will continue to be governed by the outdated provisions in RIPA. Investigators would continue to need both RIPA and the new law to make sense of the UK's surveillance landscape.

      JUSTICE considers that this is a missed opportunity.

   b. **Future-proofing?** A number of witnesses and Committee members have expressed an interest in exploring whether the Draft Bill is 'future-proof'. In our 2011 report, JUSTICE recommended that any revised surveillance framework should be flexible but robust.[492] However, we recognised that this was an area where 'future-proofing' has been notoriously difficult, not least because of the massive pace of development of new technology and how we use it in our daily lives. At the time when RIPA was passed, no one could have predicted how integrated our lives on and offline would become in such a short period. Indeed,

---

[490] *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review* (Cm 7948, October 2010), p44 (Herein the 'ISC Review' and *A Question of Trust,* David Anderson QC, June 2015 (Herein *'the Anderson Review'*). In addition, in March 2014 the then deputy prime minister, Nick Clegg MP, asked the Royal United Services Institute to coordinate a panel made up of former members of the police and intelligence services, senior parliamentarians, academics, and business people to investigate the legality, effectiveness and privacy implications of the UK's surveillance programmes. That panel reported its conclusions in July 2015: see *A Democratic Licence to Operate: Report of the Independent Surveillance Review*. Herein '*the RUSI Review*'.

[491] JUSTICE's submission to the Draft Communications Bill Committee can be read here: http://justice.org.uk/draft-communications-data-bill/

[492] *Freedom from Suspicion,* para 147. Importantly, flexibility cannot be sought at the cost of legal certainty. Overly broad powers or discretions are likely to render surveillance powers incompatible with Article 8 ECHR.

the UK has a long history of legal reform prompted by subsequent determinations that the law has failed to keep pace (from *Malone* to *Liberty v UK*).[493]

It would be regrettable if an ill-placed desire to 'future proof' these measures led to powers which were overbroad and unduly flexible. The Committee may wish instead to consider whether surveillance, by its nature, is an area suited to regular default consideration by Parliament (consider the Armed Forces Act, which must be renewed periodically). The Anderson Review made a number of recommendations to this effect, which the Committee may wish to consider.[494]

c. New powers or old?

The Government is keen to stress its view that many of the powers in the Draft Bill are already authorised by existing legislation, whether in RIPA or other provisions. Although the Home Office and the agencies may consider that powers in the Bill are both lawful and familiar, the legality of many activities is already subject to litigation in the UK and in Europe at the European Court of Human Rights and the Court of Justice of the European Union.[495]

Many of the powers in this Draft Bill are powers being considered by Parliament and the public by the first time. For example:

- *"Thematic warrants"*: Clause 13(2) provides that a Targeted Interception Warrant may apply to a single person, *or* a group of identified individuals, but can have a broader more 'thematic' application. This practice was first avowed in 2015, during the ISC Review, which discovered that the reference to a specified "person" for a targeted interception warrant under section 8(1) RIPA had been read to include, by virtue of section 81, "any organisation and any association or combination of persons". Internal guidance on this point had never been published before the ISC Review.

  In practice, this is a substantial expansion of the targeted interception warrant as debated by Parliament during the passage of RIPA. In effect, the language in Clause 13 could provide for the interception of the communications of a large category of persons, loosely defined.

- *Bulk Equipment Interference*: Clause 135 deals with warrants for bulk equipment interference. The Equipment Interference factsheet suggests that this power is not new, referencing Section 5 and 7 of the Intelligence Services Act 1994 and section 93 of the Police Act 1997 and that the practice of wide-spread use of equipment interference by the agencies and police was avowed in February 2015.

[493] *Malone v UK*, App No 8691/79, 2 August 1984, *Liberty v UK*, App No 58243/00, 1 October 2008. See *Freedom from Suspicion,* paras 59 – 61.
[494] Anderson Review, para 12.96 – 12.97.
[495] Cases currently being pursued are summarised by the Anderson Review in Chapter 5. They include *Big Brother Watch and Ors v UK*, App No 5810/73 and *Ten Human Rights Organisations v UK* (*Liberty & Ors*).

The use of this power in bulk has not yet been avowed and the conduct of bulk hacking activities remains subject to litigation.[496]

- *Data Retention and Investigatory Powers Act ('DRIPA') and communications data retention*: DRIPA was passed on an emergency timetable with extremely limited time for Parliamentary scrutiny.[497] Its measures are subject to a sunset clause which will see it lapse at the end of 2016. The provisions in Parts 3 and 4 although broadly based on DRIPA, include new features, including provision for the retention of Internet Connection Records and for the creation of "filtering" arrangements. These reflect features of the controversial Draft Communications Data Bill, previously considered and criticised by an earlier Joint Committee.

  This Bill provides a key opportunity in Parliament for detailed debate on the legal framework for the retention and processing of communications data. The foundation of these powers in DRIPA should not provide a reason to curtail full scrutiny of the justification for the powers proposed in the Draft Bill.

(c) Privacy and surveillance

9. That each of the distinct acts of collection, retention and use of personal information is engaged by our right to respect for private life, home and correspondence is trite law.[498] The protection of private correspondence is guaranteed by international and European law, including in both Article 8 of the European Convention on Human Rights and the equivalent provision of the European Charter of Fundamental Rights.[499]

10. In many instances, an individual subject to surveillance may never know whether his information has been reviewed or what has been retained. Only in the limited circumstances when the information obtained is used in a trial or when an authority acknowledges the surveillance may an individual be able to challenge its propriety.

---

[496] In ongoing litigation involving Privacy International, documents which post-date the Draft Bill express doubt on whether bulk powers are avowed or are sought anew. See: https://privacyinternational.org/sites/default/files/Schedule_Of_Public_Statements_CNE_Final.pdf

[497] Consideration of the Bill was conducted over a seven day period late in the Parliamentary term.

[498] In *Malone v UK* (1984) 7 EHRR 14, the Court considered the attachment of a 'meter check printer' to a telephone line for the purposes of recording the time calls were made, to whom and for how long. The Court considered that the collection of this information engaged the right to privacy, but in these circumstances could be justified by reference to the commercial need for a supplier of services to legitimately ensure a subscriber is charged correctly. This use was proportionate and justifiable. However, passing the information to the police without statutory authority and relevant safeguards against abuse was not. See, for example, paras 56 – 84. It is worth noting the gathering and collation of the information here is justified by the commercial need to retain information. The Draft Bill does not limit its effect to material already held by suppliers and operators, but will require the generation or retention of data not needed for any commercial purpose. The question of justification here goes to whether the generation or retention of this information can be justified for the purposes set out by the Home Office in connection with the potential for some communications to inform investigations and inquiries by public authorities. In *Amann v Switzerland* (2000) 30 EHRR 843, for example, the Court held that the storing of information about the applicant on a card in a file was found to be an interference with private life, even though it contained no sensitive information and had probably never been consulted. In Rotaru v Romania (2000) 8 BHRC 449, at para 43, the Court stressed that even 'public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities'.

[499] Article 7 CFREU. See also the International Covenant on Civil and Political Rights, Article 17.

Accordingly, in these circumstances, there is a significant obligation on the State to ensure that surveillance powers are closely drawn, safeguards appropriate and provision made for effective oversight: "*[it is] unacceptable that the assurance of the enjoyment of a right … could be…removed by the simple fact that the person concerned is kept unaware of its violation."*[500]

11. The European Court of Human Rights has stressed that the justification of any surveillance measures places a significant burden on States to adopt the least intrusive measures possible: "*[P]owers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions."*[501]

12. While safeguards are crucial to the legality of surveillance powers, they are not conclusive, nor determinative. Although the Draft Bill provides for safeguards designed to ensure that powers are applied proportionately, it is for Parliament to be satisfied that the powers *themselves* are necessary and proportionate.

13. Others are better placed than JUSTICE to provide detailed evidence on the operational case for reform and the proportionality of the powers proposed. However, we are concerned that the expansion of untargeted and bulk powers of surveillance is at odds with existing legal practice.

14. The further powers move away from traditional forms of surveillance, targeting a named individual, on the basis of reasonable suspicion that they are involved in serious criminal offending, the greater the risk to personal privacy and the broader the potential for arbitrary application and abuse. This is particularly significant in circumstances where individuals may be unable to access the mainstream justice system to challenge unlawful behaviour by public authorities or to seek redress for the violation of their individual rights.

15. Importantly, the UN Special Rapporteur on Human Rights and Counter-Terrorism had expressed concern over the breadth and impact of this kind of untargeted power: "*the use of mass surveillance technology effectively does away with the right to privacy of communications on the Internet altogether*".[502]

16. There is limited legal authority from the European Court of Human Rights to support the lawful use of such untargeted or bulk surveillance powers:

    a. Most recently, in *Zakharov,* the Court subjected a Russian law on the bulk interception of mobile phone communications to close scrutiny and found it incompatible with the right to privacy. Although provision was made in that case for judicial authorisation for access to any such material, the untargeted power

[500] (1978) 7 2 EHRR 214, paras 36, 41.
[501] Ibid, para 42. See also Para 49: *'The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism adopt whatever means they deem appropriate'.*
[502] A/69/397, paras 12.14.

was held to be incompatible with Article 8 ECHR. The measure was overbroad and subject to abuse.[503]

b. In *Digital Rights Ireland,* the Court of Justice of the European Union considered the mass retention of citizens' communications data. Testing the Data Retention Directive against a framework of safeguards, the measure was found disproportionate as it failed to make provision for specific safeguards, including, that "above all", access by national authorities was not made dependent on *"prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary."* [504]

c. In *Schrems,* the Court of Justice of the European Union stressed that "*legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life*".[505]

d. In *Liberty v UK,* the Court emphasised: "*The Court does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance on the other*".[506]

17. Beyond Europe, we note that a number of countries have recently changed their laws to restrict the ability of agencies and authorities to access communications data in bulk, including the United States, indicating that the benefit gained by such activities was minimal and disproportionate in light of the intrusion on innocent citizens lives.[507]

18. The untargeted and bulk powers in the Draft Bill must be subject to particularly close scrutiny by Parliament and an operational case for each subject to debate and test by the Committee.[508]

19. We consider below some of the new safeguards proposed in the Draft Bill.

(d) Authorising surveillance

20. The Human Rights Memorandum accompanying the Draft Bill explains the Government's view that it's primary safeguard is "the introduction of an authorisation process which includes prior approval of warrants by independent judges called Judicial Commissioners". Termed a "double-lock", JUSTICE is concerned that the Government's description of this safeguard is misleading. The provisions in the Draft Bill fall far short of

[503] *Zakharov v Russia,* App No 47143/06, 4 December 2015.
[504] *Digital Rights Ireland,* C-293/12 and C-594/12
[505] C-362/14, 6 October 2015.
[506] *Liberty v UK,* para 63.
[507] Earlier this year, bulk powers to retain telephone data in the US were allowed to lapse (Section 215, Patriot Act). This followed extensive criticism by the Privacy and Civil Liberties Oversight Board, which concluded that the material had not had a significant benefit for investigations. A number of US based intelligence professionals have expressed similar scepticism. One, William Binney, has already provided written evidence to the Committee. A similar experience occurred in Denmark, where similar bulk retention powers were judged ineffective and repealed.
[508] An operational case has been provided in the materials supporting the Draft Bill, but this only addresses the powers which relate to Internet Connection Records.

the mechanisms for prior judicial authorisation or judicial warrantry applied in other countries.

21. JUSTICE is particularly concerned that the Draft Bill: (i) conflates authorisation and review; (ii) is inconsistent in its approach to judicial involvement, (iii) provides insufficiently specific triggers for warranting powers throughout the Bill, and in particular, in connection with new thematic or bulk, untargeted powers; (iv) provides for an inappropriately broad mechanism for urgent authorisation of warrants; (v) permits the modification of warrants without sufficient oversight; and (vi) makes limited provision for to ensure that the procedure for authorisation is fair and takes into account the interests of the individual subject to surveillance and the wider community in the protection of privacy.

(i) Judicial authorisation or review?

22. The Draft Bill provides that the primary decision maker for some surveillance decisions will be the Secretary of State or a senior official, whose decision will then be subject to review by a Judicial Commissioner. The Judicial Commissioner will review whether a warrant is (a) "necessary on relevant grounds" and (b) "whether the conduct that would be authorised by the warrant is proportionate to what is sought to be achieved". In conducting a review, the Commissioner must "apply the same principles as would be applied by the court on an application for judicial review."[509] See, for example, Clause 19 (Targeted Interception, Examination and Mutual Assistance).

23. The Anderson Review recommended that all interception warrants (and bulk warrants) should be judicially authorised, concluding that "*the appropriate persons to perform this function would be senior serving or retired judges in their capacity as Judicial Commissioners.*"[510]

24. A two stage "certification" model was recommended in cases involving "defence of the UK and foreign policy". In these cases alone the Secretary of State should have the power to certify that the warrant is required in the interests of the defence and/or the foreign policy of the UK. The judge should have the power to depart from that certificate, the Independent Reviewer suggests, "*only on the basis of the principles applicable in judicial review*" which he notes would be "*an extremely high test in practice, given the proper reticence of the judiciary where matters of foreign policy are concerned*".**[511]** The judge would remain responsible for verifying whether the warrant satisfied the requirements of proportionality and other matters falling outside the scope of the certificate.

25. Unfortunately, throughout, the Draft Bill adopts a two stage process, which provides for executive or administrative authorisation, subject to judicial review. In evidence, the Government has explained its view that it is appropriate for the purposes of accountability to Parliament that the Secretary of State remain involved.

---

[509] Clause 19. However, these provisions are repeated in other clauses of the Bill.
[510] Anderson Review, para 14.47 at seq.
[511] Ibid, para 14.64.

26. In 2011, we concluded that it was this "*very accountability that leads at least some of them to disregard the rights of unpopular minorities in favour of what they see as the broader public interest. The same mandate that gives elected officials their democratic legitimacy is what makes them so ill-placed to dispassionately assess the merits of intercepting someone's communications*".[512] In practical terms, however, we note that there is, in any event, little prospect of government ministers being held to account for the interception warrants they sign so long as the details of those warrants remain secret. Among other things, Section 19 of RIPA makes it a criminal offence to disclose the existence of an interception warrant unless authorised to do so. If accountability is to be an effective safeguard, it must be more than nominal. Genuine accountability, however, would require a degree of transparency that would be impossible to square with the need for operational secrecy. If it is right, therefore, that details of interception decisions must be kept secret in order to remain effective, it would better for that authorisation to be made by someone who is already institutionally independent rather someone who is only nominally accountable.

27. A two stage model might be appropriately applied in cases involving the assessment of defence decisions and foreign policy, principally targeting communications outside of the UK. However, JUSTICE supports the original recommendation of the Anderson Review that judicial warranting should be the default mechanism for the authorisation of most surveillance decisions in the UK. The Draft Bill should be amended to provide for a single stage process of prior judicial authorisation as a default, with exception provided for a limited class subject to the certification of the Secretary of State.

28. In any event, the Draft Bill should be amended to put beyond doubt that the Judicial Commissioners must routinely conduct a full merits based assessment of necessity and proportionality:

    a. The principles of judicial review, while long-standing, are not fixed in stone, they can be altered by later judicial practice or statutory intervention (see, for example the Criminal Justice and Courts Act 2015).
    b. Since the introduction of the Human Rights Act 1998, it has been trite law that the reviewing role of any judge assessing necessity and proportionality in human rights cases *must* involve a substantive assessment.[513]
    c. However, the standard of review, even in ordinary judicial review claims, is a flexible one. In some circumstances, a reviewing court will be required to conduct 'anxious scrutiny' (for example, in cases involving breaches of fundamental rights in the common law). In other cases, the court will be expected to afford the relevant decision maker a very wide margin of discretion.[514]
    d. In a recent article, Lord Pannick QC has expressed his view that "The Home Secretary's proposals for judicial involvement *in national security cases* adopt, I

[512] *Freedom from Suspicion*, para 85.
[513] *Miss Behavin' Ltd* [2007] 1 WLR 1420
[514] See, for example, *Rehman v Secretary of State for the Home Department* [2001] UKHL 47

think, the right balance in this difficult area" (emphasis added).[515] We agree with Lord Pannick QC and the Anderson Review, as we explain above, that in *some key national security* cases the "review model" might strike an appropriate balance.

e. There is no guarantee that the close scrutiny applied in the cases cited by Lord Pannick QC will necessarily be applied to applications pursuant to the process in the Draft Bill. While this kind of anxious review has been consistently applied by the courts in cases involving threats to life or limitations on liberty, it is far from certain that this approach would apply consistently to applications following the procedure in the Draft Bill.[516]
f. Importantly, in an ordinary judicial review claim or a statutory appeal, a claimant will be able to challenge the standard of review applied in practice by a judge. Surveillance applications will necessarily be *ex-parte*. Following the procedure in the Bill, there will be no opportunity for external scrutiny of the standard applied other than in the post-hoc review by the IPC or if the Secretary of State chooses to challenge the approach of the Judicial Commissioner and request a fresh decision by the Investigatory Powers Commissioner. (In the latter case, of course, it will be open to the Secretary of State to argue that the standard of review has been *too* robust.)
g. In any event, even if close scrutiny is applied in some *national security* cases, it is unlikely that this safeguard would be sufficiently robust in others, including in the significant proportion of applications relating to law enforcement and the prevention and detection of crime.

29. We encourage the Committee to examine whether it is appropriate for Ministers to be involved at all in applications arising in the course of law enforcement operations. The Draft Bill should be amended to provide for a single step authorisation process in most circumstances, except in respect of applications involving the interference with communications of and between individuals outside the UK, engaging defence and foreign policy matters. In these circumstances, any request may be certified by the Secretary of State, subject to review by the Judicial Commissioners. However, in ordinary applications in the course of any criminal investigation, including domestic counter-terrorism activities, warrants should be subject to prior judicial authorisation alone.

---

[515] *Safeguards provide a fair balance on surveillance powers,* The Times, 12 November 2015. Lord Pannick references the involvement of courts in other decisions engaging national security. JUSTICE notes that the treatment of cases under the Terrorism Preventions and Investigation Measures Act 2012 and by the Special Immigration Appeals Commission, are not directly comparable to the ex parte application for a warrant envisaged in the Draft Bill. In those cases, albeit subject to an exceptional closed material procedure, the subject of the relevant order is aware of the proposed interference with his or her rights and can make submissions to rebut the Secretary of State's position.

[516] Consider, for example, *Home Office v Tariq* [2011] UKSC 35, [27]. The applicant sought the same guarantees applicable in TPIMs procedures – the provision of a gist of material considered in closed material proceedings. The Court distinguished this case from TPIMs determinations, which involve liberty of the individual, and similarly noted that a high standard was not expected in other significantly serious cases outside the scope of liberty claims: "Mr Tariq also has an important interest in not being discriminated against which is entitled to appropriate protection; and this is so although success in establishing discrimination would be measured in damages, rather than by way of restoration of his security clearance (now definitively withdrawn) or of his position as an immigration officer. But the balancing exercise called for in para 217 of the European Court's judgment in A v United Kingdom depends on the nature and weight of the circumstances on each side, and cases where the state is seeking to impose on the individual actual or virtual imprisonment are in a different category to the present, where an individual is seeking to pursue a civil claim for discrimination against the state which is seeking to defend itself." (JUSTICE is intervening in the case of *Tariq v UK,* currently being considered by the European Court of Human Rights).

(ii) Consistency and Communications Data

30. In any event, only some surveillance decisions in the Draft Bill benefit from any judicial involvement. There are some exemptions from review which create particular inconsistencies which the Committee might wish to consider. In others, there are differences of approach which may be difficult to justify. For example, the Secretary of State will be able to modify the terms of warrants for equipment interference by the security services without judicial approval, whereas modifications to police warrants must be reviewed by a judge.[517] There are a number of particular carve-outs for national security cases which the Committee may wish to consider. The acquisition of communications data, for the purposes of national security, does not appear, for example, to require supervision by a person independent of the application (See Clause 47(2) – (3)). Similarly constraints designed to provide limited additional protection to journalistic sources when communications data is sought will not apply to the security agencies (Clause 61).

31. All decisions on retention of communications data are taken by the Secretary of State, without provision for review (Clause 71). Access to communications data, will generally be by someone within the same organisation as the person seeking permission or by the Secretary of State (See Clause 46). A judge will only be involved in cases involving local authorities and in circumstances involving journalistic material.

32. JUSTICE considers that there is a strong case that by failing to subject retention and access to communications data to judicial oversight, the legal framework in the Draft Bill may be out of step with international standards:

    a. The Court of Justice of the European Union ('CJEU') in the *Digital Rights Ireland* decision placed a particular premium on oversight by a judicial or other independent administrative body (see above).
    b. The Government's Human Rights Memorandum appears to suggest that this decision is broadly irrelevant to the scope of domestic legislation. JUSTICE considers that this view is surprising (although we understand that the Court of Appeal has recently asked the CJEU to further elaborate on the scope of this case).[518] Not least, the analysis of the Court in respect of the kinds of safeguards necessary for the Directive, which applied across the Union, is likely to be relevant to the safeguards considered suitable for national measures. That analysis is likely to inform the consideration by national courts of necessary safeguards (see consideration by the High Court and Court of Appeal in *Davis & Watson)*[519] and by other international forums, including at the European Court of Human Rights.

[517] Clause 96.
[518] See Human Rights Memorandum, para 100. See *R (David) v Secretary of State for the Home Department* [2015] EWCA (Civ) 1185.
[519] See *Davis, Watson & Ors v Secretary of State for the Home Department and Ors* [2015] EWHC 2092 (Admin). This decision is subject to appeal and the Court of Appeal has referred a number of the questions to the Court of Justice of the European Union. See [2015] EWCA (Civ) 1185.

c. Although there is limited guidance on retention from Strasbourg, the less targeted a compulsory power exercised, the greater the likelihood the provision will be considered disproportionate. The Court has generally been hostile to the application of blanket rules applied to personal information, particularly in the criminal justice system. In *S & Marper,* for example, the Court robustly rejected domestic law on the retention of DNA and fingerprints taken from innocent adults and children. Although retention of the material served a legitimate aim – the prevention and detection of crime – its blanket application was disproportionate, particularly in light of the impact on innocent individuals and the stigma of association with a criminal database.[520] Most recently, in *Zakharov,* the European Court of Human Rights again emphasised that surveillance powers must crucially be targeted at the prevention and detection of serious crime or the protection of national security: *"Turning now to the authorisation authority's scope of review, the Court reiterates that it must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security*".[521]

33. While the legality of bulk surveillance models is currently being tested at both the CJEU and in Strasbourg, the existing case law supports an assessment that the *less* targeted the measures the *more* likely that robust authorisation and oversight measures will be necessary.

(iii) Specificity, targeting and warrants

34. The breadth of the triggers which may justify the use of the powers in the Bill and the scope of the application of individual warrants or powers require close scrutiny. In particular, the gateway to a number of thematic or bulk powers may be insufficiently precise to be compatible with Article 8 ECHR.

35. In any event, the breadth of application of some of the powers concerned may make it particularly difficult to assess necessity and proportionality in any meaningful way, undermining the ability of any authorising body, including a Judicial Commissioner to act as a significant safeguard against abuse.

36. The main grounds in the Draft Bill for issuing surveillance warrants are (a) "in the interests of national security", (b) "for the purposes of preventing or detecting serious crime" and (c) "in the interests of the economic well-being of the UK, in so far as those interests are also relevant to the interests of national security". Communications data can be accessed by a larger number of authorities and for a greater variety of purposes (including public health, public safety and for the collection of taxes, duties or levies, for example).

[520] *S & Marper v UK,* App No 30562/04, 4 December 2008.
[521] *Zakharov*, para 260.

37. While the Strasbourg court has been keen to stress that the grounds for surveillance need not be defined in absolute terms, a sufficient degree of certainty is necessary in order to allow an individual to understand when they might be likely to be subject to surveillance.

38. The Court in *Zakharov* expressed particular concern about a Russian surveillance law which permitted bulk collection of mobile telephone data for reasons connected with "national, military, economic or ecological security", noting that "*which events or activities may be considered as endangering such types of security interests is nowhere defined in Russian law*".[522] The only safeguard against abuse of this absolute discretion was effective judicial authorisation, capable of conducting a more focused assessment of the proportionality of an individual measure. However, the authorisation process in that case proved inadequate:

> *"Turning now to the authorisation's scope of review, the Court reiterates that it must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security".*[523]

39. The Court went on to conclude that the quality of review by the Russian courts was inadequate to specify the risk posed by any particular individual or the necessity and proportionality of subjecting them to surveillance, noting:

> *"courts sometimes grant interception authorisations which do not mention a specific person or telephone number to be tapped, but authorise interception of all telephone communications in the area where a criminal offence has been committed"*
>
> *"the failure to disclose the relevant information to courts deprives them of the power to assess whether there is a sufficient factual basis to suspect the person in respect of whom operational-search measures are requested of a criminal offence or of activities endangering national, military, economic or ecological security".*[524]

40. JUSTICE is concerned that a similar degree of scrutiny is likely to be impossible, or at least exceptionally difficult, when applied in the context of the thematic or bulk powers in the Draft Bill, which may apply to ill-defined categories or groups of people (or to the communications of most individuals in the UK, provided they are using particular services based outside the United Kingdom, like Facebook or GMail).[525] For example, the Draft Equipment Interference Code of Practice, explains that individuals who are "not intelligence targets in their own right" may be the subject of warrants for thematic equipment interference.[526]

---

[522] *Zakharov,* para 246.
[523] *Zakharov,* para 260.
[524] *Zakharov,* paras 265 and 261.
[525] The Anderson Review notes that the consideration of the existing RIPA model in *Kennedy v UK* considered targeted surveillance, not bulk measures of the kind contemplated in the Draft Bill. See para 5.43.
[526] Draft Code of Practice on Equipment Interference, February 2014, Home Office.

41. In these circumstances, the ability of a judicial authorisation procedure to reliably test necessity and proportionality of the impact of a measure on an individual is likely to be inherently limited, and as such, is unlikely to operate as a significant safeguard against abuse.

(iv) Urgency

42. Throughout the Draft Bill judicial review is accompanied by an alternative 'urgent' procedure (see for example, Clause 20). The scope of the urgent mechanism is extremely broad and ill-defined, and in our view could fatally undermine any safeguard provided by any mechanism for judicial authorisation or review.

43. The Bill provides that a urgent warrant by be issued by the Secretary of State in any case which she "considers" there is "an urgent need". Urgent need is not defined. An urgent warrant must be subject to judicial review within 5 days. If a judge is satisfied that the surveillance should never have been authorised, they may (but are not required to) order that the material gathered is destroyed.

44. JUSTICE considers that this provision is unnecessary and would permit the already limited judicial scrutiny proposed in the Draft Bill to be side-stepped in ill-defined circumstances and for unspecified purposes.

45. JUSTICE recognises that surveillance decisions may be required urgently. However, urgent decision-making would be familiar to any judge or former judge appointed as a Judicial Commissioner. From search warrants pursuant to the Police and Criminal Evidence Act 1984 to High Court duty judges dealing with injunctions and deportation, urgent orders in family cases for child protection, considering evidence and taking decisions on short notice at anti-social hours forms a familiar part of the judicial experience. There are a number of provisions for warrantry in connection with the investigation of serious crime (including terrorist offences), and no concern has been raised about the inability to raise a judge an appropriate hour to allow an investigation to continue without undue delay.[527] There are likely to be multiple Judicial Commissioners capable of serving on a duty rota. In practice, urgent decision making is likely to be less of a burden for the cadre of Commissioners than for a single Secretary of State.[528]

46. Very recent guidance from the Grand Chamber of the European Court of Human Rights affirms that this kind of urgent model is likely to be inadequate to protect the privacy rights of individuals subject to surveillance. In *Zakharov,* the Court considered an urgent authorisation mechanism in operation in Russia, which provided for administrative authorisation, with independent review within 48 hours. Even in these limited circumstances, the Court was extremely critical of the use of broad and ill-defined discretions to trigger an emergency procedure: "*The domestic law does not limit the use*

[527] For example, Section 40, Terrorism Act 2000 requires a search warrant to be issued before premises can be searched in connection with terrorist offences in the Act

[528] The Committee has already heard evidence about the strain placed on Ministers by the warranting process. This burden was key in the Independent Reviewers conclusion that judicial warrantry was necessary in the new legislative framework. See *Anderson Review*, para 14.54.

of the urgency procedure to cases involving an immediate serious danger to national, military, economic or ecological security. It leaves the authorities an unlimited degree of discretion in determining in which situations it is justified to use the non-urgent judicial procedure, thereby creating possibilities for abusive recourse to it".

47. While the proposals in this Draft Bill provide for subsequent review within five days there is no clear requirement for material to be destroyed, even if the material is gathered unlawfully, or for steps to be taken to provide redress for the unlawful surveillance conducted. Instead those matters remain within the discretion of the individual Judicial Commissioner, who must hear arguments from the Secretary of State, subject to appeal to the Investigatory Powers Commissioner. We are concerned that this model creates little disincentive against abuse of the urgent procedure.[529]

(v) Modification

48. JUSTICE is concerned about the breadth of provision in the Bill for warrants to be modified after the authorisation process is complete. These provisions are not consistent in their application throughout the Draft Bill and it is far from clear why the Government considers such broad provision for self-authorised modification might be appropriate.[530] Clause 26, for example, provides that Targeted Interception, Targeted Examination and Mutual Assistance Warrants, including those thematic warrants targeting groups of persons or places, could be modified by the Secretary of State or a senior official at any time, to add or remove any person, place or organisation. It would also permit a minor modification by the person to whom the warrant is addressed, or their colleagues, to vary such names or descriptions or to add, vary or remove any other "factor" specified in a warrant. These modifications can be made without any further judicial authorisation.[531] JUSTICE is particularly concerned that this broad power could entirely side-step the limited judicial oversight provided in this part of the Bill.

49. The breadth of such modification provisions are of particular concern in the context of "thematic interception warrants" or any bulk warrant in the Draft Bill. For example, clause 13 makes clear that Targeted Interception Warrants may cover not only identified individuals or premises, but may also cover groups of persons sharing a common purpose or activity as well as or more than one set of premises or organisations, where

[529] See *Zakharov*, [266] and *Association for European Integration and Human Rights and Ekimhzhiev* App No 62540/00, 28 June 2007, [16]. By contrast in this latter case, the Court considered a Bulgarian law, which allowed for an urgent warrant subject to review and authorisation by an independent judge within 24 hours. The power was only available in circumstances where there was an "immediate risk that a serious intentional offence would be committed" or "an immediate threat to national security". In this case, the reviewing judge had the discretion to decide whether material obtained should be retained or destroyed. Yet, the Court only accepted this procedure on credible evidence that the use of this power was intended to be "used sparingly and only in duly justified cases" (para [82]). The relevant law was found incompatible with the right to respect for private life for other reasons (it failed to provide for subsequent oversight, notification after-the-event, and adequate provision for access to redress).

[530] For example, in connection with the provision in the bill for equipment interference – hacking – different authorisation models apply to hacks by the security agencies or the police. The agencies are authorised by warrant from the Secretary of State, subject to judicial review, police hacks are self-authorised within the force, subject to judicial review. Modifications minor and major – including to names, places and conditions – can be made by the Secretary of State without review. Modifications to police warrants must be subject to judicial review. See Clause 96.

[531] By way of contrast, Clause 96, which deals with the modification of warrants for equipment interference, provides that any modification which would have been subject to judicial approval on application cannot take effect without judicial authorisation. See Clause 96(6).

these are part of the same investigation. The legality of this kind of untargeted surveillance remains untested, and has only recently been avowed (during the course of the ISC inquiry). If the modification power in Clause 26 applies to thematic interception; as it appears it must, this could, for example, mean a warrant for interception of the communications of a group of students at the University of London could, in principle, be legitimately expanded to cover all students in the UK without further judicial approval.

50. In *Zakharov,* the Grand Chamber not only confirmed the importance of independent judicial authorisation, it made clear that part of the value of the safeguard lay in ensuring legal certainty about the scope of warrantry.[532]

51. JUSTICE considers that *any* substantive change to a warrant should be subject to fresh judicial approval. The Draft Bill should be amended accordingly.

(vi) Procedural matters

52. Firstly, the Draft Bill should be amended to make clear that a security-vetted Special Advocate should be appointed to represent the interests of the subject and the wider public interest as necessary. For the past 15 years, it has been a statutory requirement in Queensland to appoint a Public Interest Monitor to supervise all applications for the use of surveillance devices.[533] In October 2011, Victoria also introduced a Public Interest Monitor in respect of applications for interception and surveillance.[534] In March 2015, the Australian federal government announced that it would introduce a Public Interest Monitor in relation to applications for access to journalists' communications data.[535]

53. Secondly, it should be open to the Judicial Commissioners to issue clear guidance on the law and its application. This could be achieved, for example, by permitting Judicial Commissioners to produce reasoned decisions on a point of law or principle, in any particular application, subject to anonymisation and redaction as necessary to protect sensitive material damaging to national security. The recent experience of the IPT in publishing judgments on law and principle might inform this process.

54. Finally, if the Draft Bill retains the two-stage 'review' model, it should be made explicit that all the material provided to the Secretary of State on application for the relevant warrant (together with any relevant updating material) must also be provided to the Judicial Commissioner.

55. While the Government has again compared Communications Data – including the collection of new ICR data – to a telephone bill, the reality is that this material is far more intrusive. In its unanimous decision in the 2014 case of *Riley v California*, for instance,

---

[532] See [264] – [265]: "As regards the content of the interception authorisation, it must clearly identify a specific person to be placed under surveillance or a single set of premises…". Notably, the Anderson Review would have required all substantive changes to warrants to be subject to judicial authorisation. See Recommendations 34, 39 and 49. This would have included, particularly, any change to names or premises.

[533] See Police Powers and Responsibility Act 2000 (Qld) s 740(1) and Crime and Misconduct Act 2001 (Qld) s324(1).

[534] Public Interest Monitor Act 2011 (Vic).

[535] See e.g. "Abbott government and Labor reach deal on metadata retention laws", Sydney Morning Herald, 19 March 2015.

the US Supreme Court noted that mobile phones "*place vast quantities of personal information literally in the hands of individuals*".[536] Indeed, Chief Justice Roberts remarked that: "*it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives— from the mundane to the intimate*".[537] That record includes not just the *content* of communications but also, the Court held, the data relating to those communications, e.g. a person's search history and location data.[538] The Court went on to approve Justice Sotomayor's 2012 description of GPS data as producing "*a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations*".[539]

56. Officials, agencies and others have expressed concern about the administrative burden that judicial oversight of communications data retention and requests for access would create. However, different models might be considered to accommodate the bulk of requests for communications data. In *Freedom from Suspicion,* we recommended that certain types of data (including basic subscription data) might be exempt from prior judicial authorisation when sought by law enforcement agencies or the emergency services.[540] The Anderson Review would have subjected 'novel or contentious' access requests to judicial oversight.[541] An alternative means to reduce the administrative burden could be to subject requests for communications data to judicial oversight by *specially trained* magistrates, operating as part of the IPC. We consider this recommendation in some detail in *Freedom from Suspicion: Second Report.*[542]

(e) The Investigatory Powers Commission

57. One of the key recommendations of *Freedom from Suspicion,* in 2011, was the need to both strengthen and streamline the existing oversight arrangements for the use of surveillance powers by public bodies. In the first instance, we recommended that

---

[536] 573 US (2014) per Roberts CJ at 9.

[537] Ibid, 19. The Chief Justice also noted that the very term "*cell phone*" was itself "*misleading shorthand*" since "*many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers"* (ibid, 17). Before mobile phones "*a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy*" simply because *"[m]ost people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read*", whereas "*the possible intrusion on privacy is not physically limited in the same way when it comes to cell phones*" (ibid, 17-18).

[538] For example, "*[a]n Internet search and browsing history … can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building*".

[539] 565 US (2012) at 3, cited at *Riley*, ibid, at 20.

[540] *Freedom from Suspicion*, para 182-186.

[541] Both the ISC and RUSI reports acknowledged the sensitivity of communications data. For its part, the ISC sought to distinguish "basic" data used to identify the "who, when and where" of a communication from what it described as "communications data plus", which would encompass "details of web domains visited or the locational tracking information in a smartphone". It suggested that, whereas basic data did not require the same protection as the content of communications, there were nonetheless "legitimate concerns" that "communications data plus" had "the potential to reveal details about a person's private life (i.e. their habits, preferences and lifestyle) that are more intrusive" and therefore required greater safeguards (though it did not spell out what those safeguards should be).

[542] *Freedom from Suspcion: Second Report,* para 27.

increasing the use of prior judicial authorisation would significantly reduce the need for ex-post facto oversight as well as the burden on the IPT.

58. More generally, however, we observed that the oversight arrangements under RIPA were unnecessarily complex and ineffective: in the case of encryption notices under Part 3, for instance, responsibility for oversight is spread across three different commissioners: the Intelligence Services Commissioner (where the notice is sought by the intelligence services), the Chief Surveillance Commissioner (where the notice is sought by the police) and the Interception of Communications Commissioner (if the notice relates to intercepted communications). We recommended, therefore, that the oversight functions of the Interception of Communications Commissioner and the Intelligence Services Commissioner should be transferred to the Office of the Chief Surveillance Commissioner, with that body assuming sole responsibility for the oversight of surveillance powers by the police, intelligence services and other law enforcement bodies.

59. Against this background, we welcome the provision in the Draft Bill to consolidate the responsibilities of the diverse commissioners in a single Investigatory Powers Commission ('IPC'). However, whether that body succeeds in becoming a robust, transparent and accountable public facing body, which increases public confidence, will depend very much on its structure, powers and resources. We are concerned that provisions in the Draft Bill may inhibit the independence of the IPC or limit its effectiveness in practice. We address a number of concerns, below.

(i) Resources

60. The effectiveness of the IPC and the confidence of the public will hinge not only on the independence of the body and the powers granted by Parliament, but on the resources available to it. We share the concern expressed by Sir Stanley Burnton that the budget holder for the Commission will be the Secretary of State whose conduct – or the conduct of agencies or bodies for which she is responsible - will be subject to its scrutiny.[543] Even in circumstances where a more diffuse overlap between the conduct of an auditing body and its sponsoring department exists, Parliament has previously expressed concern about conflicting interests (see, for example, the Justice Select Committee's examination of the Information Commissioner's independence and budget, which recommends that body should report to, and be funded by Parliament).[544] In light of the significance of the role to be played by the IPC, and the very substantial overlap between its scrutiny function and the work of the Secretary of State, there is, in our view, a strong case for a different funding model.

61. In any event, given that Judicial Commissioners will be drawn from the pool of judicial expertise and may be former – or sitting – senior judges, the judiciary or Her Majesty's Courts and Tribunals Service should be involved in or consulted about budget setting for the IPC. Importantly, if a number of judges are to be drawn away from the High Court to sit as part of the IPC, this reduces the capacity of the High Court which should

[543] Q 56, HC 651, 2 December 2015.
[544] See Ninth Report of 2012-13, *The functions, powers and resources of the Information Commissioner,* paras 28 – 31.

accordingly be compensated by the Treasury to maintain its capacity. Judicial Commissioners should not be appointed at cost to the wider judicial system.

(ii) Independent and effective?

62. We are concerned that the Bill replicates the language and model adopted by RIPA, focusing on the "Commissioner" rather than the Commission. This may appear a superficial distinction, but the structure of the Commission may be crucial to its success in practice. Not least, it appears from the face of the Bill that the Government intends to conflate the judicial and the inspection and audit functions of the Commission within the responsibilities of the Judicial Commissioners.

63. Clause 169 sets out the main oversight functions of the "Commissioners". In Clause 169, the Draft Bill places a broad duty on Judicial Commissioners not to act in a manner which is contrary to the public interest or prejudicial to national security, the prevention and detection of crime or the economic well-being of the United Kingdom. We regret the inclusion of this duty in the Draft Bill. It appears, at best, superfluous, in light of the functions of the IPC, and at worst designed to encourage a degree of deference within the Commission towards the assessment of the Secretary of State and individual agencies and bodies of the risks associated with their work. However, that this Clause distinguishes between warranting (where the duty will not apply) and the wider functions of the Commissioners suggests that the Commissioners will be undertaking both judicial and audit functions.

64. Plainly, the credibility of the Judicial Commissioners may be reduced if they appear to be "checking their own homework". The conflation of the judicial and inspection roles within the Commission is inappropriate, reduces the objective independence of the Judicial Commissioners and could undermine the effectiveness of the IPC model.

65. In *Freedom from Suspicion: Building a surveillance framework for a digital age,* we explained our view that:

> *"There are plainly considerable advantages to all the relevant expertise being combined within a single body, and the involvement of judicial commissioners will go a long way towards helping to establish its institutional independence. As for the concern about combining authorisation and oversight within a single body, we do not see grounds for particular concern. As the Independent Reviewer noted, the Office of the Chief Surveillance Commissioner already performs authorisation and oversight functions in respect of Part 2 of RIPA[545] and there has been no criticism of that model that we are aware of. On the contrary, we consider that there are likely to be significant benefits from having a pool of judges with expertise in surveillance matters, supported by an independent body with the high level of technical and cross-disciplinary expertise that will be necessary to provide effective scrutiny in this fast-changing field."[546]*

[545] *Anderson Review*, para 14.98.
[546] *Freedom from Suspicion: Second Report,* para 47.

66. Our view is based on the consideration that, within a single organisation, the judicial and audit functions within the body would remain operationally distinct (See Annex 17, Anderson Review, for example). While the Judicial Commissioners would benefit substantially from being able to draw upon the technical expertise open to inspectors and auditors, we are concerned that the conflation of roles in the Draft Bill would undermine both judicial independence and public confidence in the IPC. If their functional independence cannot be maintained within the IPC model, another structure may be more appropriate.

67. In the interests of maintaining the independence of the Commission, the Investigatory Powers Commissioner and the Judicial Commissioners should be subject to an appointment mechanism which is beyond reproach. We are concerned that the Draft Bill provides for an appointment by the Prime Minister alone, although the IPC should be consulted. At the very least, we would expect the Lord Chief Justice to be involved in, or consulted on, a judicial appointment of this nature. However, we recommend that each of these appointments is made by the Judicial Appointments Commission ('JAC'). While we welcome the provision in the Bill for these appointments to be drawn from those who have already held high judicial office; we consider that suitability for appointment *to these particular posts* should be tested in an open and transparent way, best managed by the JAC.

(iii) Powers and responsibilities

68. Clause 169 of the Draft Bill sets out the main oversight functions of the Investigatory Powers Commissioner. Clause 169(1)-(3) creates a very broad duty to keep "under review" the exercise by public authorities of various statutory functions under this Bill and under RIPA, the Police Act 1997 and the Intelligence Services Act 1994. This reviewing power will "include" "audit, inspection and investigation".

69. On 2 November 2015, following a roundtable conducted by JUSTICE and King's College London, the Interception of Communications Commissioners Office ('IOCCO') produced a "wish-list" for any new single body.[547] These included the power to conduct investigations and thematic inquiries at their own instigation and the power to refer specific cases to the IPT for determination. This reflects our recommendations in *Freedom from Suspicion* that any consolidated body should be able to refer cases directly to the IPT and that the oversight of surveillance should be designed to address thematic problems and to provide for more wide-ranging inquiries about the effectiveness of the law.[548]

70. The Draft Bill should be amended to put beyond doubt the capacity of the IPC to conduct inquiries on its own initiative about the operation of the legal framework within its sphere of responsibility. While this power might be used sparingly within the resources available, it could be extremely effective in identifying good practice and areas where

[547] http://www.iocco-uk.info/docs/Kings%20College%20Round%20Table.pdf

[548] Although in our first report, we recommended that the IPT should adopt responsibility for these more thematic inquiries, it would be entirely proper for the new IPC to have this inquisitorial role.

the law remains uncertain. We return to the relationship between the IPC and the IPT, below.

71. Section 170 creates a power for the Prime Minister to direct the IPC to conduct a review of any aspect of the functions of the intelligence services, the head of any such service or any part of the armed forces or MoD in so far as they are conducting intelligence activities. It is unclear how this power is intended to be exercised and how far this kind of investigation might be designed to replace or supplement inquiries by the Intelligence and Security Committee or public inquiries into matters of public importance relating to the conduct of the intelligence services or the armed forces. As the Bill provides for the scope of such inquiry to be determined by the Prime Minister, who is also permitted to redact any conclusions of an inquiry by the IPC, its output may be of limited value for the purposes of meeting any responsibility on the part of the Government to conduct an independent, effective and transparent inquiry (including, for example, in connection with an Article 2 ECHR obligation in any case where deaths have resulted).

72. Clause 172 stipulates particular duties for the Judicial Commissioners in connection with the work of the IPT. This includes providing assistance and advice to public bodies and others within their sphere of responsibility and to the IPT, including on cases live before the Tribunal (echoing Recommendation 117 of the Anderson Review). We welcome the acknowledgment that the Commissioners and the IPC might have a role in providing advice or guidance on the application of the law. However, the Committee may wish to consider whether the relationship between the IPC and the IPT is properly drawn. The IPT may ultimately take decisions on the lawfulness of decisions by the Commissioners. We are particularly concerned that, in any circumstances where the Judicial Commissioners are giving their view on the law, they may be required to first consult with the Secretary of State (Clause 172(3)). This could undermine the apparent independence of the Judicial Commissioners.

73. The Draft Bill makes no provision, beyond error notification (see below), for the IPC to refer an issue directly to the IPT. In circumstances where apparently unlawful conduct is identified in the course of an investigation or an audit, or inconsistency in the application of the law, it may be helpful for the IPC to refer an issue directly to the IPT. This could be particularly useful where an issue affects a group or class of individuals unlikely to pursue an individual claim before the Tribunal; or in circumstances where the interpretation of the law or its application to a new practice may be in doubt.

74. Finally, we regret the very broad provision for the functions and powers of the IPC to be amended by Ministers in secondary legislation (Clause 171(9)). The limited capacity for Parliamentary scrutiny of secondary legislation makes this power inappropriate. The existence of this power endangers the apparent independence of the Commission and its effectiveness as a safeguard against abuse.

(iv) Notice and redress

75. Clause 171 provides a mechanism for the IPC to report errors to the IPT. The IPC must report to the subject of any surveillance any "relevant error" which it considers is a

"serious error". The individual will only be informed if the IPT agrees it is a "serious error" and it is in the public interest for the person concerned to be informed.

76. While we recommended in *Freedom from Suspicion* that errors should be notified to the IPT and the individual concerned, there are a number of significant problems with this measure:

    a. We understand that, in practice, IOCCO already reports errors relating to communications data where relevant, in which case, this provision would constrain existing practice through the addition of new qualifiers and limitations on reporting. The Draft Bill includes an express bar on reporting of any other errors except by virtue of Clause 171 (Clause 171(9));
    b. The Draft Bill defines the seriousness of any error by reference to the impact on the individual concerned, without reference to the illegality of the conduct by the relevant public body. Any reportable error must, in the view of the Commissioner, have caused "significant prejudice or harm to the person concerned" (Clause 171(3)). This would significantly limit the circumstances when the duty to report is triggered, despite unlawful conduct by a public body inspected by the IPC.
    c. This "serious error" benchmark is set disproportionately – and inappropriately – high by the Draft Bill. Clause 171(4) indicates that something *more* than a breach of Convention rights protected by the HRA 1998 is required for an error to be considered "serious".
    d. If the purpose of reporting is to allow an individual to consider whether to pursue a case before the IPT, it is unclear why reports should be limited only to cases of serious error. The Bill provides a detailed mechanism for reporting on serious errors and the maintenance of relevant data about reported errors (Clause 171(10)). We are concerned that the distinction between serious and other errors could, in practice, lead to underreporting of surveillance inconsistent with the requirements of the law or the relevant Codes of Practice. This could significantly diminish the effectiveness and value of the new IPC.

77. This provision falls far short of the mandatory notification requirements which operate in other countries. The Bill should be amended to give the IPC a duty to notify any relevant person of any error discovered in targeted surveillance, except in circumstances where disclosure would risk any on-going operation or investigation, or otherwise endanger national security or the prevention and detection of crime.

78. We consider that the Draft Bill should additionally be amended to provide for a *default* mandatory notification mechanism.[549] The requirement for individuals to be notified of surveillance as soon as possible, is a key safeguard identified by the European Court of Human Rights, which as stressed that *"as soon as notification can be made without jeopardising the purpose of the surveillance after its termination, information should be provided to the persons concerned".*[550] The House of Lords Constitution Committee has

[549] *Freedom from Suspicion,* para 389.
[550] See *Association for European Integration and Human Rights and Ekimhzhiev* App No 62540/00, 28 June 2007, para [90]-[91

previously recommended that *"individuals who have been made the subject of surveillance be informed of that surveillance, when completed, where no investigation might be prejudiced as a result".*

79. Provision for mandatory notice would allow individuals to pursue a claim before the IPT in their own right even in circumstances where the IPC has not identified an error. This model operates in other countries without difficulty, and although notification in very sensitive cases may be less likely, the potential for disclosure may create an additional impetus towards lawful decision making by agencies and other bodies exercising these compulsory powers. For example, for instances of interception in law enforcement matters in the United States, notification is by default within 90 days of the termination of the relevant surveillance, unless the authorities can show there is "good cause" to withhold that information.[551] A similar model operates in Canada, where the subjects of interception warrants for the purposes of law enforcement must be given notice within 90 days of a warrant expiring. This may be extended up to three years in terrorism claims, subject to judicial oversight, if in the "interests of justice".[552] We understand that similar models apply in both Germany and the Netherlands, with similar exemptions to protect the integrity of ongoing inquiries.[553]

(v) Disclosure, cooperation and whistle-blowing

80. While we welcome a number of measures in the Draft Bill designed to protect against abuse of power, we are concerned that prohibitions on disclosure should not inadvertently discourage or prevent individuals within public authorities or agencies or in CSPs from approaching the IPC with concerns or communicating with the Commission frankly.

81. Notably, Clause 8 provides for an offence of unlawfully obtaining communications data. Clause 43 prevents individuals from disclosing whether an intercept warrant is in place, or its terms. Clause 66 makes it an offence for telecommunications operators or their employees to disclose any information about the requirements imposed on them in connection with communications data or access to that data. Although Clause 43 makes provision for an authorised disclosure to a "Judicial Commissioner", this exception is not consistently applied to all non-disclosure duties and offences in the Bill. (We address our concerns about the scope of the role of the Judicial Commissioner, above).

---

[551] 18 U.S.C §2518 (8) (d). See Annex 15, Anderson Review, for a brief analysis of comparative practice in the "five eyes" jurisdictions.

[552] Section 188, 195-196, Canadian Criminal Code.

[553] Under the German Code of Criminal Procedure, section 101(4)(3), individuals under telecommunication surveillance shall be notified of surveillance measures. The notification should mention the individual's option of court relief and the applicable time limits and should be given as soon as possible without "endangering the purpose of the investigation, the life, physical integrity and personal liberty of another or significant assets including the possibility of continued use of the undercover investigator." But notification will be "dispensed with where overriding interests of an affected person that merit protection constitute an obstacle." In the Netherlands, under the Code of Criminal Procedure, Part VD, Chapter One, Section 126bb, the public prosecutor must notify in writing the user of telecommunications or the technical devices of the surveillance "as soon as the interest of the investigation permits", but not if it is not reasonably possible to do so. If the individual is a suspect and learns of the exercise of surveillance power through means described in 126aa(1) or (4) of the Code, notice is not required. If the inquiry relates to an investigation of terrorist offences or another serious offence, information pertaining to an individual's name, address, postal code, town, number, and type of service of a user of a communication service may be requested, and the notice provisions of 126bb will not apply.

82. In light of the history of significant misunderstandings and disagreements about the scope of surveillance law, it would be regrettable if individuals and organisations were prevented from consulting with the IPC about good practice and legality by overly rigid non-disclosure requirements. It must be open to individuals – in either public bodies or CSPs – to ask the IPC for guidance and draw their attention to areas of conflict in the application of the law. This might be particularly helpful where there is a disagreement between different public bodies, or between a CSP and a public agency, about the precise scope of the powers circumscribed. Similarly, a safe-route to the IPT for would-be whistle-blowers wishing to report bad practice should be clear and accessible. This could be achieved by inserting a provision into Part 8 specifying that any disclosure to the IPC for the purposes of soliciting advice about any matter within the scope of its responsibilities, or for the purposes of supporting its duty to review, will be an authorised disclosure, not subject to any criminal penalty.

(f) The Investigatory Powers Tribunal

83. Four years ago, we regretted the difficulty of bringing a claim before the Investigatory Powers Tribunal ('IPT') and the limited form of redress available before the Tribunal. We made a series of recommendations concerning the role of the IPT:

    a. oversight commissioners should have the power to refer cases to the IPT for investigation whenever he or she reasonably suspects that a public authority has acted unlawfully, including the unnecessary and disproportionate use of surveillance powers;[554]

    b. mandatory notification periods should be specified in law (see above);[555]

    c. the investigative capabilities of the Tribunal should be increased and extended to enable it to undertake proactive investigations arising from any systemic failings identified by the relevant oversight commissioner, or in cases where there are reasonable grounds to suspect the unauthorised use of surveillance by a public body;[556]

    d. the Tribunal should adopt internal procedures to increase adversarial testing of relevant evidence, including the appointment of a standing panel of special advocates to represent the interests of the excluded party in any case where the Tribunal's investigations have identified a case to be answered;[557] and

    e. the existing policy of Neither Confirm Nor Deny ('NCND') should be relaxed sufficiently to enable the Tribunal to adopt fair procedures (including the right to

[554] *Freedom from Suspicion*, para 397.
[555] *Freedom from Suspicion,* para 396.
[556] *Freedom from Suspicion*, para 398.
[557] *Freedom from Suspicion*, para 399.

an oral hearing, disclosure of evidence, cross examination of witnesses and the giving of reasons).[558]

84. In the wake of the Snowden disclosures, the IPT considered a number of complaints concerning the activities of the intelligence services. In addition, complaints have been brought concerning the use of surveillance powers to identify journalists' sources. In 2015, the IPT delivered no less than three judgments identifying a breach of Convention rights:

    a. In *Liberty and others v GCHQ and others (No 2),*[559] the Tribunal held that, prior to its disclosure of the relevant internal arrangements for the handling of such material, the legal regime governing the intelligence services' receipt of communications intercepted by foreign intelligence services had not complied with the requirements of legal certainty under Articles 8 and 10 ECHR;

    b. In *Belhaj and others v Security Service and others*,[560] the IPT held that the legal regime governing the interception of legally privileged material was not in accordance with the law under Article 8(2) ECHR; and

    c. In *Liberty and others v GCHQ and others (No 3)*,[561] the IPT held GCHQ's interception of the private communications of two human rights organisations – the Egyptian Initiative for Personal Rights and the Legal Resources Centre – had violated their rights under Articles 8 and 10 ECHR. Several days later, however, the Tribunal notified the parties via email that it had made a mistake in its determination, and that it was Amnesty International and not the Egyptian Initiative that had been the victim of unlawful interception.

85. In the first instance, the three cases show the importance of notification of surveillance. In our 2011 report, we noted that it was no coincidence that half the successful complaints to the IPT involved cases where the complainants had been notified that they had been subject to surveillance. So too in the cases of *Liberty and others* and *Belhaj*, but for the disclosure of Edward Snowden as to the activities of the UK's intelligence services, the complaints would never have been brought and the public at large would have had no inkling that the legal framework was not compatible with the requirements of the Convention.

86. In its recent report, the ISC praised the Tribunal as "*an important component of the accountability structure*" but recommended the introduction of a domestic right of

---

[558] *Freedom from Suspicion*, para 400. Since our recommendation in 2011, we note that the doctrine of NCND has come under some judicial criticism in recent years: see e.g. the speech of Maurice Kay LJ in *Mohamed Ahmed Mohamed and CF v Secretary of State for the Home Department* [2014] EWCA Civ 559 at para 20 ("It is not simply a matter of a governmental party to litigation hoisting the NCND flag and the court automatically saluting it") and that of Bean J in *DIL and others v Commissioner of Police of the Metropolis* [2014] EWHC 2184 (QB) para 42 ("just as (in the well-known words of Page Wood V-C in *Gartside v Outram* (1856) 26 L.J.Ch 113) "there is no confidence as to the disclosure of iniquity", so there can be no public policy reason to permit the police neither to confirm nor deny whether an illegitimate or arguably illegitimate operational method has been used as a tactic in the past").

[559] [2015] UKIPTrib 13_77-H, 6 February 2015.

[560] [2015] UKIPTrib 13_132-H, 13 March 2015.

[561] [2015] UKIPTrib 13_77-H_2, 22 June 2015.

appeal against its decisions.[562] The RUSI panel described the Tribunal as "*a work in progress*" and made several criticisms of its procedures, including that the Commissioners have no power to refer cases to the Tribunal;[563] secondly, that its rulings were frequently "*opaque*";[564] that its reliance on complaints brought by the public "*was not a helpful or just arrangement*";[565] and that its recent confusion between Amnesty International and the Egyptian Initiative for Personal Rights pointed to the need for "*clear procedural improvements that will need to be implemented*".[566] It also endorsed the need for a domestic right of appeal.[567]

87. For his part, the Independent Reviewer noted that the Tribunal was operating increasingly in the open and was "*likely increasingly to be perceived as a valuable and effective check on the exercise of intrusive powers*".[568] He supported the introduction of a right of appeal on points of law and changes to enable the IPT to make declarations of incompatibility pursuant to Section 4, HRA 1998.[569] Notably, the Independent Reviewer declined to make any recommendations concerning the Tribunal's procedures, indicating that this was an issue for argument on "another day" (outside the scope of his inquiry).[570]

(i) Appeal rights

88. Clause 180 introduces a right of appeal from the IPT "on a point of law", subject to certification by the IPT or the appropriate appeal court. JUSTICE welcomes the introduction of this right of appeal. We are concerned however that it appears that the Draft Bill would only provide for appeals against a final *determination*, not in respect of interim legal findings during the conduct of the proceedings. This could lead to unfairness and wasted resources as proceedings may continue to a full determination, on the basis of an error in law, only to result in an appeal at a later stage.

89. Clause 180 provides that the route of appeal will be determined by the Secretary of State in regulations, with such cases as determined to be heard by a specified court in Scotland or Northern Ireland, or in other cases by the Court of Appeal. JUSTICE considers that delegation of this kind is inappropriate. Routes of appeal should be specified on the face of the Bill.

(ii) IPT and procedural reform

90. JUSTICE regrets that the Draft Bill takes no further steps to increase the openness and effectiveness of the IPT and the ability of individuals to secure redress for unlawful acts of public surveillance. We consider this a missed opportunity:

---

[562] *ISC Report*, para 217LL.
[563] *RUSI Report*, para 4.87.
[564] Ibid, para 4.89.
[565] Ibid, para 4.88.
[566] Ibid, para 4.94.
[567] Ibid, para 4.86.
[568] *Anderson Review*, para 14.102.
[569] *Anderson Review*, recommendation 114 and para 14.105.
[570] *Anderson Review*, para 14.108.

a. **Notification:** We consider the limited provision for notification in the Draft Bill, above. We consider that a default statutory framework for the after-the-event notification of individuals subject to surveillance would significantly improve the likelihood that individuals are able to pursue their claims before the IPT. As explained above, while the IPT has worked hard during the past year to eighteen months, the bulk of this work as arisen as a result of the Snowden revelations. Without the objects of surveillance having knowledge that a claim may be appropriate, it is unlikely that the workload of the Tribunal will be sustained.

b. **Procedures and openness:** Like the Independent Reviewer, we welcome the Tribunal's recent efforts to improve the transparency of its procedures. Those efforts, however, remain very much bound by the constraints imposed by RIPA and the Tribunal's ability to set its own procedural rules. The Committee has received direct evidence from others, including Amnesty International, on the opaque nature of proceedings in the Tribunal. Nothing in the Draft Bill would address the inherent limitations in the procedures before the IPT.

   In light of the consensus across each of the three reviews – ISC, Anderson and RUSI – towards greater openness before the IPT, we recommend that the Draft Bill is amended to provide that all proceedings before the IPT should be open, unless a closed material procedure can be justified in the public interest.

   This approach would test the boundaries of the blanket "*Neither Confirm nor Deny*" ('NCND') principle. Although the Tribunal has found a means to work around the application of NCND, by proceeding on the basis of assumed facts, the limitations of this approach have become apparent during the course of the preparation of the Draft Bill. In the litigation preceding the introduction of the Bill, the Government has incurred significant litigation costs refusing to confirm, nor deny, certain practices by the security agencies, which have now been avowed in connection with the passage of this Bill (some as late as in the material accompanying its publication).[571]

c. **Adversarial testing/Special advocates:** JUSTICE considers that the Bill should be amended to make clear that in any closed session, a Special Advocate is appointed to allow any case to be subject to adversarial testing. However valuable the role played by counsel to the Tribunal in closed proceedings, it is not an effective substitute because counsel to the Tribunal is *not* charged with representing the interests of the excluded party and, in the *Liberty* case, counsel took no instructions from the excluded parties.

   Parliament should take this opportunity to specify – whether in the model of a Special Advocate - or through an express obligation to appoint a Counsel to the Tribunal – that any claimant's interests should be represented in closed session by a security vetted counsel and the case of the public agency concerned subject to adversarial scrutiny.

[571] See *Freedom from Suspicion,* 392 – 393, *Freedom from Suspicion: Second Report,* paras 39 – 40.

While JUSTICE has principled concerns over the expansion of the use of secret evidence, such limited scrutiny and representation offered by a Special Advocate should not be limited to the discretion of any individual court, but available as of right in any case involving a closed material proceeding, including before the IPT.[572]

d. **Human Rights Act 1998:** The Bill should be amended to implement the Anderson Review recommendation that the IPT should be empowered to make a declaration of incompatibility pursuant to Section 4, HRA 1998. While the right to appeal will ensure that a declaration might be sought before the Court of Appeal, the Tribunal should have the opportunity to consider whether a declaration would be appropriate. It would be an inefficient use of judicial resources if the only reason an appeal might be pursued would be to secure a remedy unavailable at first instance.

(g) Privileges

91. JUSTICE is concerned that the treatment of important legal privileges, and notably, legal professional privilege, in the Bill is cursory. The Bill provides that where the correspondence of Members of Parliament (or Members of the Scottish Parliament, the Welsh Assembly and the Northern Ireland Assembly) is subject to targeted interception or a request for access to communications data, the Secretary of State must consult the Prime Minister before granting the relevant warrant (Clauses 16 and 85). Clause 61 provides that access to communications data *for the purpose of* targeting journalistic sources must be authorised by a Judicial Commissioner. The only reference to legal professional privilege is in Schedule 6, which provides that the Code of Practice on Communications Data will make provision for any particular considerations relevant to legally privileged information (Schedule 6 (4)).

92. In *Freedom from Suspicion,* JUSTICE regretted that the treatment of legal professional privilege under RIPA had been inadequate and that the Codes of Practice produced under its various parts had provided little reassurance to the public that communications which benefitted from privilege were being handled lawfully.[573] In the interim, domestic court decisions have confirmed that the treatment of privileged material under the RIPA framework has been far from certain either for the agencies or the beneficiaries of the relevant privileges.[574]

(i) Legal Professional Privilege

93. JUSTICE shares the concerns expressed by the Bar Council, the Law Society of England and Wales and others, that in order to afford proper respect to legally privileged material, the Draft Bill must be amended.[575]

---

[572] See *Freedom from Suspicion,* para 378 – 392; *Freedom from Suspicion: Second Report,* para 41.
[573] *Freedom from Suspicion,* paras 110 – 115, 339 – 342.
[574] See, for example, *Belhadj,* [2015] UKIP Trib 13_132-H, *Lucas, Jones and Galloway v SSHD & Ors,* [2015] UKIPTrib 14_79-CH. See also, *R v Barkshre* [2011] EWCA Crim 1885.
[575] See, for example, Draft Investigatory Powers Bill, Parliamentary Briefing, Bar Council, November 2015; Investigatory Powers and Legal Professional Privilege, Bar Council, Faculty of Advocates, The Bar of Northern Ireland and The Law Society

94. Legal professional privilege is a core principle at the heart of any effective justice system, designed to preserve access to justice and the rule of law. By ensuring that individuals are able to take legal advice in confidence, without fear of interference, the rule preserves the right of persons to access the law fully and fairly. This principle is one respected in democratic countries the world over. It rightly exists to protect the rights of the client, not the interests of the legal professional. Thus, privilege can only be waived with the consent of a client. The European Court of Human Rights has stressed that surveillance measures which might endanger professional privilege will require additional safeguards.[576] Each of the three reports – ISC, Anderson and RUSI – recognise the importance of privileges and confidence in connection with surveillance powers.[577]

95. The material which accompanies the Bill explains the Government's view that the Part 3 Code of Practice, dealing with communications data, will require applicants for a warrant seeking access to data containing legally privileged material to provide a "compelling case".

96. JUSTICE considers that this approach falls far short of the provision necessary to preserve client confidence in legal professional privilege:

    a. Codes of Practice are subject to limited Parliamentary scrutiny. Although they might be approved by Parliament, as delegate legislation, they are unlikely to be subject to detailed debate, and MPs and Peers will have no opportunity to provide for their amendment;

    b. The existing Codes have proved an unsatisfactory bulwark against abuse (see *Belhadj* (IPT). The revised versions are also likely to provide a similarly limited safeguard;[578]

    c. While Draft Codes are unavailable for review, any model which permits surveillance of legally privileged material would be overbroad and inconsistent with the spirit of the existing case law.

       Although the House of Lords accepted that RIPA might permit the interception of legally privileged materials in *Re McE,* the conclusions in that case are limited and controversial. In light of the long standing protection for legal professional privilege offered in centuries of common law, and in statute (for example, in the Police and Criminal Evidence Act 1984), the decision was a surprise to practitioners and commentators alike. The case considered an analysis of a part of RIPA which did not expressly mention legal professional privilege, nor which

---

of England and Wales, October 2015; and Response to the Joint Committee on the Draft Investigatory Powers Bill, The Odysseus Trust (Office of Lord Lester of Herne Hill QC), 15 December 2015.

[576] *Niemietz v Germany* [1992] 16 EHRR 97; *Kopp v Switzerland* App No 23224/94.

[577] *ISC Report*, Chapter 10(d), p95; *Anderson Review*, para 2.12, *RUSI Review*, para 2.10.

[578] Notably, these Codes proceed on the basis that interference with legally privileged material is authorised by RIPA. See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473845/6.1276_151104_INTERCEPTION_CoP_for_designer_FINAL_WEB.PDF. This Code was laid before Parliament on 4 November 2015; at the time of writing it was not yet approved.

Parliament had considered. In any event, the decision should be narrowly confined to truly exceptional circumstances and subject to the highest possible safeguards. For example, Lord Carswell considered "grave and imminent threats" alone, such as the killing of a child or an imminent terror attack, might justify interference with legal privilege.[579] Equally, Lord Phillips indicated the importance of prior judicial authorisation, indicating that the European Court of Human Rights would require at a minimum that interference with privileged material should be governed by a clear statutory framework, providing the limited circumstances where privilege might be overridden and access to person with "judicial status" to determine any such question.[580]

It is clear that the Draft Bill contains no such limitations.

d. The approach in the Draft Bill would offer *less* protection to legally privileged material than to the protection of journalistic sources or to the communications of Members of Parliament. Of all the privileges considered in connection with the Draft Bill, the case for the protection of legally privileged material is beyond question. That it is the only privilege not afforded specific protection on the face of the Draft Bill is regrettable.

97. Broadly, in our view:

a. The Bill must acknowledge that the protection of legal professional privilege is important for *all* forms of surveillance, including bulk forms of activity.

The Draft Bill currently confines its provision to the treatment of communications data. It makes no mention of the privilege in connection with retention of data; or methods which might in practice be *more* intrusive, including targeted interception warrants and forms of equipment interference.

b. There should be a clear statutory presumption that legally privileged material should not be deliberately targeted for surveillance. This should only apply to material which attracts privilege. Where privilege is lost or set aside, including in circumstances where a lawyer is complicit in unlawful behaviour ('the iniquity exemption'),[581] the bar should not apply.

c. If there are any circumstances where material which might be legally privileged may be sought (e.g. in reliance on the 'iniquity principle'), this should be subject to clear prior judicial authorisation, not Ministerial or official authorisation subject to subsequent judicial review (see above).

[579] See *Re McE* [2009] 1 AC 908, [108]
[580] See *Re McE* [2009] 1 AC 908, [41]
[581] See for example, Police and Criminal Evidence Act 1984, Section 10(2). Importantly, it appears that the Government does not seek to target LPP, but only the circumstances when it may be abused. If this is the case, then there should be no objection to amendment of the Draft Bill to exclude deliberate targeting of legally privileged material in applications, as abuse of the kind envisaged would abrogate the privilege concerned. See 30 November 2015, Evidence of Paul Lincoln, Q 15, HC 651, 30 November 2015.

d. Codes of Practice for each of the powers granted in the final Bill should be required to provide guidance to prevent, in so far as possible, the inadvertent capture of legally privileged material, and to ensure that if captured, such data is afforded such additional protection as necessary to ensure respect for access to justice and the rule of law. The Bill should be redrafted to specify that the purpose of any guidance in the Code should be designed to protect against the unlawful disclosure of privileged material.

(ii) The 'Wilson' Privilege/Journalistic sources

98. JUSTICE considers that the other privileges in the Bill should be subject to a similarly comprehensive approach. We are concerned about the inconsistency of approach in the Draft Bill. Thus, additional protection is afforded to Members of Parliament subject to a targeted interception warrant, but not to journalists seeking to protect their sources. Similarly, while access to communications data which targets journalistic sources provides for authorisations to be subject to judicial review, access to other communications data, which might engage the privilege afforded to Members of Parliament or to legally privileged material is not.

99. There are some wider concerns about these provisions, which the Committee might wish to consider. For example, will consultation with the Prime Minister provide significant reassurance for members of parties in opposition? Similarly, will such consultation garner much reassurance outside Westminster, if at all? In considering the sanctity of communications with members of the Scottish Parliament and the Welsh and Northern Ireland Assemblies, members might with to consider whether consultation with the Prime Minister would give any comfort.

100. The Committee may wish to ask the Government to explain the inconsistency in approach to each of the privileges considered in the Draft Bill, and to explain a) why the safeguards afforded to each might differ; b) why those safeguards might be different for different kinds of surveillance; and c) why the protection offered should not be specifically determined by Parliament on the face of the Bill.

(h) Intercept as evidence

101. Clause 42 of the Draft Bill, together with Schedule 3, broadly replicates the existing procedure in Section 17(1) of RIPA, whereby material obtained by way of an intercept warrant cannot be used as evidence in ordinary criminal proceedings. Schedule 3 makes a number of exceptions to allow intercept evidence to be considered in civil proceedings where a closed material procedure – where a party and his or her legal team are excluded – is in place. These proceedings, for example, include proceedings under Section 6 of the Justice and Security Act 2015, in the Special Immigration Appeals Commission or under the Terrorism Prevention and Investigation Measures Act 2011. There is no exemption for criminal proceedings, except in so far as material may be disclosed to the prosecution and to the judge, in order that a judge might determine

whether admissions by the Crown are necessary in order for the trial to proceed in a manner which is fair; (if it would not be fair, a prosecution may have to be dropped).[582]

102. JUSTICE has long recommended the lifting of the bar on the admission of intercept material as evidence in civil and criminal proceedings. In 2006, we published *Intercept Evidence: Lifting the ban,* in which we argued that the statutory bar on the use of intercept as evidence was 'archaic, unnecessary and counterproductive'.[583] The UK's ban reflects a long-standing Government practice but it is out of step with the position in many other commonwealth and European countries and it has proved increasingly controversial over time. Importantly, the ECtHR has recognised the value placed on admissible intercept material, in countries where it is available, constitutes 'an important safeguard; against arbitrary and unlawful surveillance, as material obtained unlawfully will not be available to found the basis of any prosecution.[584] In 2014, a Privy Council review confirmed that fully funded model for the removal of the ban could result in a "significant increase in the number of successful prosecutions".[585]

103. The Targeted Intercept Factsheet produced by the Government to accompany the Draft Bill, states:

> *"Intercept material cannot be used as evidence in criminal proceedings. Successive Governments have reviewed whether it would be possible to introduce intercept as evidence. Each has concluded that it would not be possible - the Agencies' abilities to conduct the investigations that we rely on to keep us safe would diminish."* [586]

104. This reflects the position in the latest Privy Council review, which concludes that complying with existing disclosure requirements and preparation for trial would be administratively difficult and costly. Since the precise benefit in increased successful prosecutions cannot be quantified, there will be no change in position unless law enforcement budgets could be increased:

> *"the increased resource burden would mean either that a very large amount of other agency activity was dropped to fund intercept as evidence or that interception would be available for many fewer investigations or both."*[587]

105. David Anderson QC considered that the ban on intercept evidence was not within the remit of his review. He did, however, note that "*the relative impact of interception is probably in decline, as communications data become more abundant*". He acknowledged CPS evidence that the bar on intercept material meant that communications data was of increasing importance in securing prosecutions.[588]

---

[582] See Schedule 3(21).
[583] See JUSTICE, *Intercept Evidence: Lifting the ban*, October 2006, p13 – 17. See also *Freedom from Suspicion,* paras 129 – 139.
[584] *Uzun v Germany,* App No 35623/05, [72].
[585] *Intercept as Evidence*, Cm 8989, December 2014, para 84. The review also reflected the concerns of the agencies and law enforcement bodies that removing the ban without full funding could reduce their effectiveness.
[586] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473739/Factsheet-Targeted_Interception.pdf
[587] *Intercept as Evidence,* Cm 8989, December 2014, paras 86 - 91.
[588] *Anderson Review*, para 9.16 – 9.18.

106. As our 2006 report made clear, the experience of other countries shows that the fears of the intelligence services about the operational impact of using intercept as evidence is ill-founded. Intercept evidence has been admissible for many years in such common law countries as Australia, Canada, New Zealand, South Africa and the United States. Not only do all these countries share the same adversarial legal system as our own, but they have similar disclosure requirements to those required in England and Wales.[589]

107. The failure of this Bill to reconsider the role of intercept material as evidence would represent a missed opportunity for Parliament to bring UK practice into line with the approach in other countries; a step which consensus agrees could lead to more successful prosecutions against those guilty of terrorist offences and other forms of serious crime. The Committee may wish to consider how the bar on the use of targeted intercept material relates to a new focus on expanded and untargeted access to communications data; and whether lifting the ban (a) would increase the likelihood of successful criminal prosecutions, (b) would reduce reliance on administrative alternatives to prosecution, such as Terrorism Prevention and Investigation Measures Orders ('TPIMs') or on the use of untargeted forms of surveillance, and (c) whether the costs based analysis conducted by the Government is accurate and sustainable.

5 January 2016

[589] *Freedom from Suspicion,* para 138.

Mr. Bernard Keenan, Dr. Orla Lynskey, Professor Andrew Murray—written evidence (IPB0071)

Introduction and Executive Summary

This submission is in the form of four collected briefing papers prepared by members of the Law Department of the London School of Economics and Political Science (LSE). These papers were prepared to give an academic analysis of key sections of the draft Investigatory Powers Bill in the hope this may frame the policy discussion. Each section is circa four pages and is therefore hopefully digestible to the very busy committee members. The sections are:

- Ensuring the Rule of Law (Professor Andrew Murray and Mr. Bernard Keenan)
- Comparing Surveillance Powers: UK, US, and France (Professor Andrew Murray)
- Bulk Personal Datasets in the draft Investigatory Powers Bill (Mr. Bernard Keenan)
- Beyond privacy: the data protection implications of the IP Bill (Dr. Orla Lynskey)

We make a number of key observations on the draft Bill to the joint committee:

- It is vital that any state that passes invasive surveillance powers does so with due regard to the fundamental rights of its citizens. [1.1]
- It seems clear that the ordinary meaning of Cl. 19(2) is that the Judicial Commissioner will be asked to review the Secretary of State's action in issuing a warrant on Judicial Review principles alone. A Commissioner will be prevented from fully assessing the necessity and proportionality of warrant applications unless they are provided a full and frank assessment of all material facts and are able to request, and receive, further information from the agency bringing the request. [1.7]
- The double-lock system proposed simply does not offer the judicial independence required by the rule of law, while the closed system of hearings used by the IPT fails to ensure that justice shall be seen to be done in public. [1.12]
- By taking bold decisions, such as the passing of the USA Freedom Act 2015, the public confidence and the capacity of the Federal Government in protecting both the liberties and safety of its citizens is enhanced. While provisions similar to those proposed in the draft IP Bill in place already in France have failed to make France or French citizens any safer. If we in the UK follow the French lead we will be no safer but we will lie in a less liberal state. [2.11]
- The decisions and risk factors produced by analysis of Bulk Personal Datasets threaten personal autonomy and risk producing systemic discrimination, stereotyping, and biased decisions, both at the policy level and operational level. Individuals at home in the UK or abroad will have no control over the type of processing of their personal information that the agencies carry out for authorized purposes. This may lead to operational or policy decisions that profoundly affect that individual without their knowledge or consent. Data analytics is not a neutral process. Before a dataset can be analysed for patterns, an analyst must define the terms of interest. How these terms are defined has a huge impact on the results observed. Yet the intelligence services necessarily operate in secrecy. Non-transparency means that where innocent people may be flagged up for attention, such as further surveillance or equipment interference, they will not be able to seek

redress unless the IPC is able to investigate and inform them after the fact. [3.15 – 3.17]

- 'Mission creep' is a real concern. The point of gathering and analysing bulk data is to identify hitherto unknown patterns. By nature, it is a speculative exercise. The temptation then is towards 'total' interception of data in order to meet the lawful objective, as all data is *potentially* useful. Thus General Keith Alexander's alleged instruction to the NSA to 'collect it all'. [3.18]
- The right to data protection also protects data security. Data security is described as the 'essence' of the right to data protection in the judgment of the CJEU in *Digital Rights Ireland*. It would therefore appear that to comply with the right to data protection, data processing operations – such as those envisaged by the IP Bill – must have technical and organizational measures in place to tackle the destruction, loss or alteration of data. [4.8]
- At present in the UK, SIAs rely on a 1994 Act to hack equipment including computers, laptops and mobile devices. The IP Bill provisions dealing with 'Equipment Interference' provide a more explicit legal basis for this hacking. These provisions are unlikely to comply with the data security requirement of the right to data protection [4.9]
- Following the judgment of the Court in *Digital Rights Ireland*, the UK was concerned that the legal basis for its existing data retention legislation was in doubt and it enacted new legislation (the Data Retention and Investigatory Powers Act (DRIPA) 2014). This legislation, which will expire at the end of 2016, was challenged before the High Court on the grounds that it was incompatible with the findings in *Digital Rights Ireland*. The High Court agreed, albeit on the basis of a very narrow interpretation of the ECJ's judgment. The High Court finding was then appealed to the Court of Appeal, which has stayed the proceedings in order to refer a number of questions to the ECJ. In particular, the Court of Appeal wishes to ascertain whether – contrary to the findings of the High Court – the shortcomings of the Directive highlighted by the ECJ in its judgment constitute mandatory requirements which national legislation must respect. The answer to this question will be critical to the validity of the IP Bill. [4.12]
- Since the CJEU's findings, constitutional courts in Austria, Slovenia, Belgium, Romania and Slovakia as well as a district court in the Netherlands have found national data retention to be incompatible with the judgment and thus invalid. The UK may soon find itself in an isolated position. If the UK is one of few EU Member States which obliges communications service providers to facilitate equipment interference, companies will move their manufacturing and technological operations elsewhere. [4.16]

Part I: Ensuring the Rule of Law (Professor Andrew Murray and Mr. Bernard Keenan)

The Investigatory Powers Bill must reconcile the increase in invasive surveillance powers with the rule of law. Crucially, Parliament must ensure that it allows the institutions that play a vital part in its functioning, such as judicial commissioners and the Investigatory Powers Tribunal, are given the capacity and autonomy to meet the appropriate standards of transparency and judicial independence.

1.1 It is vital that any state that passes invasive surveillance powers does so with due regard to the fundamental rights of its citizens. While the nature of covert surveillance implies that those subject to surveillance cannot know they are under surveillance, it is vital that in undertaking covert surveillance, including the interception and the gathering and retention of data, the rule of law is upheld. A number of fundamental rights, including the right to freedom of expression, the right to privacy, the right to a fair trial, the principle of non-discrimination, the presumption of innocence, and the right to an effective remedy risk being infringed by the increase in surveillance powers. Citizens should be aware of the legal basis upon which the interception and retention of data is undertaken. In the past the UK has been accused of lacking transparency in this regard with equipment interference provisions covertly authorised under s.5 of the Intelligence Services Act 1994, while the Investigatory Powers Tribunal ruled that bulk receipt and storage by GCHQ of data gathered by the National Security Agency in the United States was in breach of the right to freedom of expression and the right to privacy. The ruling highlighted the lack of accessible indication to the public of the legal framework and the absence of legal safeguards. Moreover, it was only with the introduction of the Investigatory Powers Bill that the Home Secretary avowed that s.94 of the Telecommunications Act 1984 has been used to justify bulk collection of communications data. This has been described by Amberhawk Training, the UK's leading information law training provider, as the exercise of powers "in a way that were never subject to Parliamentary scrutiny… neither subject to the relevant Code of Practice covering communications data nor to scrutiny from the Regulator who was specifically tasked by Parliament to supervise the use of communications data." It is imperative that one of the outcomes of the Investigatory Powers Bill is legal transparency and the re-invigoration of the rule of law in this sphere.

1.2 This paper looks at three aspects of the involvement of judges in the regulation of investigatory powers as proposed in the draft bill. First, it places the bill in the context of the growth of secrecy in the legal system. Second, it explains the role of judges in the authorisation of interception warrants. It then turns to the role of the Investigatory Powers Tribunal in reviewing complaints about the legality of the use of such powers.

The Rule of Law and secrecy

1.3 The role of Judicial Commissioners is novel, but must be placed within recent developments that have brought state secrecy within the parameters of the legal system. Beginning with the Interception of Communications Act 1985, it has become possible to legally challenge the government's use of interception powers. Interception powers are by nature secret: they lose their efficacy otherwise. Therefore legal procedures have been developed that are partially carried out behind closed doors, without disclosing the full content of the government evidence revealed during such 'closed' hearings. Such 'closed' hearings have transformed the nature of the judicial task. Until recently it was taken for granted that an open, adversarial system of justice should always be transparent with equality of information between parties, but that is not the case when hearings are 'closed'. So-called 'closed' proceedings began in immigration proceedings but have developed into different areas of public law, including civil damages claims, care proceedings, employment tribunal hearings, and review of the use of interception powers. The Judicial Commissioners proposed in the bill represent a new forum in which the judiciary is asked to cross the

'waterline' between secrecy and transparency. This creates a troubling challenge to the doctrine of separation of powers, drawing judges into the realm of executive decision-making and threatening the impression of impartiality on which the legal system ultimately depends.

Authorisation: the 'Double Lock' Provision

1.4 Since 1656, interception of communication has been lawful only where it has been authorised by a ministerial warrant. This is in contrast to the position in other democracies such as the United States, where judges and not politicians take such decisions. This is a key area of concern in the draft bill. Although David Anderson QC recommended that interception warrants and communications data warrants should be approved only by judge rather than the Home Secretary, the draft Bill proposes instead the 'double-lock' model as proposed by RUSI. As has been pointed out by a number of commentators, including the Shadow Home Secretary, it is not clear by any means that the double-lock provisions found in the Bill, wherein warrants are issued by the Secretary of State or relevant Scottish Minister, subject to a judicial review by a judicial commissioner before coming into effect, meet the Anderson/RUSI requirements for judicial oversight. Anderson recommended that "specific interception warrants, combined warrants, bulk interception warrants and bulk communications data warrants should be issued and renewed only on the authority of a Judicial Commissioner." RUSI was less bullish in recommending "where a warrant is sought for purposes relating to national security (including counter-terrorism, support to military operations, diplomacy and foreign policy) and economic well-being, the warrant should be authorised by the secretary of state subject to judicial review by a judicial commissioner". It is clear that the proposed role for the Judicial Commissioner under the Bill is the much lower RUSI level of responsibility, this is despite Anderson warning that "to pass muster under EU law, the UK rules that replace DRIPA 2014 s1 and the Data Retention Regulations 2014/2042 will have to be prefaced at the very least by consideration of: (c) prior authorisation by a judicial authority or independent administrative body".

1.5 Additionally it has been pointed out that the double lock system is deficient in at least two ways. The Bar Council have pointed out that "the 'double lock' requirement … is not as secure as it is made out to be. Government ministers will be able to authorise the interception of people's conversations and messages in 'urgent cases' - defined as up to five days without authorisation - where judicial approval is not possible. It is likely that a high volume of requests to snoop on people's conversations will have an element of urgency about them. Excluding judicial authorisation under any circumstance immediately removes the element of independent oversight. As all lawyers know, there is a duty judge available through the Royal Courts of Justice 24 hours a day. There is no reason why such provision could not be made available in cases where investigatory powers are being sought."

1.6 More immediately worrying for any effectiveness of the double lock system is the nature of the review that the Judicial Commissioner will carry out. MP David Davis and campaigner Shami Chakrabarti have pointed out that in effect the Judicial Commissioner will only be ensuring that proper procedure has been followed. Mr. Davis commented "I draw everybody's attention to section 19(2), which tells the judicial commissioners they have to make decisions based on judicial review principles, not on the basis of the evidence. In other

words the home secretary would have to behave in an extraordinary manner not to get his or her warrant approved. This is not the judge checking the evidence, it is the judge checking that the correct procedure has been followed. This is not quite the protection it was represented as." Ms. Chakrabarti commented "there is no judicial authorisation for interception in this Bill. At most, there is a very, very limited role for judges in a rubber-stamping exercise. It is not judicial sign-off, it is not acceptable in a modern democracy ...They have spun it as a double lock, but the second person, the judge, does not actually have a key." Interestingly David Anderson does not agree: "the Bill also contains safeguards. My report, and that of RUSI, were particularly influential here. There will be a powerful, outward-facing super-regulator, and save in urgent cases, no warrant will enter into force without judicial approval – a reversal of consistent practice since at least the 17th century."

1.7 It seems clear that the ordinary meaning of Cl. 19(2) is that the Judicial Commissioner will be asked to review the Secretary of State's action (or the action of any other relevant person) in issuing a warrant on Judicial Review principles alone: this is whether the action was (a) illegal; (b) unfair (illegitimate); or (c) irrational or disproportionate. It seems this will be extremely difficult for the Commissioners to decide on these matters unless they have access to all the data that the Secretary of State disposed of when making the initial decision. A Commissioner will be prevented from fully assessing the necessity and proportionality of warrant applications unless they are provided a full and frank assessment of all material facts and are able to request, and receive, further information from the agency bringing the request.

1.8 Finally we note that by way of Cls. 169(5) & 169(6) Judicial Commissioners are warned that they "must not act in a way which is contrary to the public interest or prejudicial to — (a) national security, (b) the prevention or detection of serious crime, or (c) the economic well-being of the United Kingdom, and that a Judicial Commissioner must, in particular, ensure that the Commissioner does not — (a) jeopardise the success of an intelligence or security operation or a law enforcement operation, (b) compromise the safety or security of those involved, or (c) unduly impede the operational effectiveness of an intelligence service, a police force, a government department or Her Majesty's forces." Though thankfully these clauses are not applied when they are fulfilling their double-lock functions, the intent of the role of Judicial Commissioner is set out in statutory language. But this clause has the effect of requiring a Judicial Commissioner to either agree or disagree with the political decision taken by Home Secretary. This implicitly politicises the judicial role, unless it is strictly limited to assessing the procedural form, rather than the actual substance, of the warrant in question.

Review – the Investigatory Powers Tribunal

1.9 The draft bill Investigatory Powers Tribunal (IPT) was created to operate not as an adversarial court, but as an inquisitive body, set up to provide a means of redress where an individual or organisation believes that they have been subjected to unlawful use of investigatory powers. In its ordinary operation, complaints can be submitted to the Tribunal on a standard application form. Assuming the complaint is not vexatious or fanciful, judicial members of the IPT then meet privately, obtain evidence from the agencies implicated, and reach one of two possible outcomes; 'Complaint Not Upheld' or 'Complaint Upheld'. Where

a complaint is upheld, unlawful surveillance has occurred. A limited report is provided to the complainant and a full account is sent privately to the Prime Minister. To date there has been only one such finding against the intelligence services. 'Complaint Not Upheld' applies where there has been lawful surveillance or no surveillance whatsoever, so as to maintain the ambiguity over the use of the power where it may be deployed. Thus a limited form of redress exists while maintaining official secrecy.

1.10 However the IPT also holds the power to determine its own proceedings under s.68 of RIPA. Where a complaint raises a general point of law, the IPT conducts an open hearing to publicly hear arguments in an adversarial format and to clarify the law. The government's position in such procedures is to maintain a 'Neither Confirm Nor Deny' stance over all operational matters, meaning the case proceeds on the assumption that the alleged powers of interception are being used, determining the law as it ought to apply were the facts correct. But proceedings have also the use of 'closed' hearings as outlined above. The effect is that that the government is both able to maintain a position of detachment with respect to the facts of the case, while also revealing privately to the Tribunal the reality of the operational position. To manage this process, an *ad hoc* 'Counsel to the Tribunal' has been created by the IPT to intervene and advise the Tribunal. The Counsel to the Tribunal is a security-vetted lawyer. In the IPT their role is inquisitive and advisory.

1.11 The overall effect is that the parties bringing the case to the IPT do not have their position put to the Tribunal in a partisan, adversarial manner during 'closed' sessions, so that the government is able to unilaterally decide during proceedings how much information ought to be disclosed into the public domain. This hybrid manner of proceeding creates serious problems for the separation of powers and the perception of judicial independence. It is therefore imperative that the structure of the mechanisms for redress and review are clarified and judicial independence is secured in the IPT.

Conclusions

1.12 It is in the nature of covert surveillance that it is in the interests of law enforcement agencies and the security services to have maximum freedom to operate with minimal public knowledge of their activities and with light touch oversight. It is argued that this freedom to operate hidden from the sight of the public allows them to carry out their duties more effectively. This argument seems to have held sway with successive UK governments who have allowed both law enforcement agencies and the security services to operate with little publicity of their powers and operational capacity and little public oversight. The publication of the Snowden documents revealed just how little we knew. The draft investigatory powers bill is in the governments own words an attempt to bring clarity and oversight to the operation of covert surveillance and data retention by drawing together a number of disparate powers and authorisations into one overarching legal framework. However there is still much to be done to protect and enshrine the rule of law in UK surveillance activity. We remain concerned that an independent judiciary are not at the heart of the warrant issuing process. The double-lock system proposed simply does not offer the judicial independence required by the rule of law, while the closed system of hearings used by the IPT fails to ensure that justice shall be seen to be done in public. We welcome the moves made in the draft bill towards greater transparency and a new rule for judicial

commissioners in the warrant granting process, however the draft bill falls far short of what we would expect in an open democratic society living under the rule of law.

Part II: Comparing Surveillance Powers: UK, US, and France (Professor Andrew Murray)

How to best structure surveillance powers in the Investigatory Powers Bill? What can we learn from the experience, institutional choices and structures adopted in the United States of America and in France? This section of the brief gives a short overview of the different choices and experiences in the US and France, and explains what we can learn from the contrasting models adopted in those countries.

Overview

2.1 Both France and the US operate an extensive signals intelligence network, not unlike the UK's, and both have experienced recent terrorist activity and remain likely targets for terrorist activity in the future, like the UK. At the same time, the US and France have a divergent approach to the legal framework for surveillance powers. The US is taking steps to reduce the legal authority of Federal bodies, including national security bodies, to intercept and retain communications data and content. France, on the other hand, has recently substantially extended authorisation and powers for interception and retention of data. In institutional terms, the the United States operates a judicial authorisation process while France operates a political authorisation process, which is not unlike the double-lock process proposed in the Investigatory Powers Bill.

The United States

2.2 US citizens are protected from the unreasonable interference by the state into their privacy by the Fourth Amendment to the US Constitution. Against this backdrop, federal warrants to intercept communications may only be obtained under three federal statutes: the Omnibus Crime Control and Safe Streets Act of 1968, the Foreign Intelligence Surveillance Act of 1978 (as amended by the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008) and the Communications Assistance for Law Enforcement Act (CALEA) of 1994. Title III of the Omnibus Crime Control and Safe Streets Act pertains mainly to lawful interception during criminal investigations. This requires Federal, state and, other government officials to obtain judicial authorisation for intercepting wire, oral, and electronic communications such as telephone conversations and e-mails. FISA governs wiretapping for intelligence purposes where the subject of the investigation must be a foreign (non-US) national or a person working as an agent on behalf of a foreign country. The FISA court issues these warrants judicially. CALEA covers public broadband networks and Internet access and Voice over IP services that are interconnected to the Public Switched Telephone Network (PSTN) – again through a judicially authorised warrant.

2.3 In the 2000s, surveillance focus in the US turned to terrorism. NSA warrantless surveillance outside the supervision of the FISA court caused considerable controversy. It was revealed in 2013 that since 2007, the National Security Administration had been collecting connection metadata for all calls in the United States under the authority of §215 of the USA Patriot Act of 2001, with the mandatory cooperation of phone companies and

with the approval of the FISA court. The Federal Government maintains it does not access any information in its own database on contacts between American citizens without a targeted, judicial warrant.

2.4 The Federal Government of the United States has taken significant steps to curtail the surveillance powers of the state and to provide greater oversight in recent months. The USA Freedom Act of 2015, which replaces the USA Patriot Act of 2001, has made significant moves to protect the American people from bulk surveillance and data collection. §201 of the Act prohibits the bulk collection of data by trap and trace (a system to record all incoming communications data) and pen register (a system which records all outgoing communications data), including bulk communication data collection by the NSA. Bulk surveillance of Internet metadata is still permitted by §702 of the FISA Amendments Act of 2008, although this must be targeted only at non-Americans. There are two specific protections for American citizens contained in the Act: (1) the Federal Government is specifically prohibited from intentionally targeting American citizens under §702, and (2) it has a sunset provision of 31 December 2017. While it is likely that §702 may be renewed in some fashion after this deadline, the fact that §215 of the USA Patriot Act was not renewed in the USA Freedom Act (which had been the basis of the NSA's programme of collecting all Americans' calling records) indicates that the political debate over §702 may be significant and controversial. The Electronic Frontier Foundation, for example, has campaigned against its renewal on the basis that "while targeting others, the NSA routinely acquires innocent Americans' communications without a probable cause warrant."

2.5 The final part of the triumvirate (now duumvirate following the repeal of §215) of Federal Surveillance powers is Executive Order 12333, originally passed by President Reagan in 1981. This provides that "agencies within the Intelligence Community shall use the least intrusive collection techniques feasible within the United States or directed against United States persons abroad. Agencies are not authorized to use techniques such as electronic surveillance, unconsented physical search, mail surveillance, physical surveillance, or monitoring devices unless they are in accordance with procedures established by the head of the agency concerned and approved by the Attorney General. Such procedures shall protect constitutional and other legal rights and limit use of such information to lawful governmental purposes." In other words, the constitutional protections of the Fourth Amendment apply throughout. In the post Snowden environment, the movement in the legal oversight regime in the United States has clearly been towards greater transparency, less reliance on bulk data gathering (for domestic investigatory purposes) and oversight by independent judicial officers.

France

2.6 If we are to make a comparison with a relevant European power, we must compare our position to France. This is due to the considerable rhetoric in the media that the UK needs the powers contained in the Investigatory Powers Bill to keep its citizens safe in light of the tragic events in Paris on the evening of 13 November 2015. This has been a regular theme in the media in the immediate aftermath of these events. Examples include Lord Carlile's essay for the Mail on Sunday and the Prime Minister's comments on the Today programme on 16 November. When one looks at French law in this area, we see that France already has most of the legal powers the Government seeks to introduce or entrench via the Bill. Yet these

powers tragically failed to prevent the attacks of 13 November. The relevant French powers are mostly contained within the Loi du 24 Juillet 2015 relative au renseignement (Law of 24 July 2015 relating to intelligence). The Law, passed quickly following the Charlie Hebdo attacks in January, was criticized by human rights groups and technology companies for being rushed through without proper consultation or scrutiny.

2.7 The law relating to intelligence provides the French State with a set of legal rights not dissimilar to the Bill. The law creates a framework in which the intelligence services are authorised to have extensive access to information technologies. Intelligence gathering techniques that are allowed include: tagging vehicles, capturing images in private places, network access to telecommunications operators data for tracking individuals identified as posing a terrorist threat, and a requirement that Internet Service Providers install "black boxes" to monitor users. Following an amendment by the Assemblée Nationale, ISPs are required to separate off connection data from content. Intelligence services can only see connection data. The law allows the Prime Minister to authorise intrusive surveillance measures for broad and undefined goals such as "major foreign policy interests", protecting of France's "economic, industrial and scientific interests" and prevention of "collective violence" and "organised delinquency". It even has an equivalent to the dual-lock system proposed in the Bill. The Commission Nationale de Contrôle des Techniques de Renseignement (CNCTR) (National Intelligence Oversight Technical Commission) checks the Prime Minister's actions.

2.8 CNCTR succeeds the Commission Nationale de Contrôle des Interceptions de Sécurité (CNCIS) (the National Security Interceptions Control Commission). The CNCTR consists of 13 members: 3 members of the State Council, 3 judges from the Court of Cassation, an expert in electronic communications appointed on a proposal from the state telecoms authority, and 6 parliamentarians (3 Deputies and 3 Senators). CNCTR fulfils a role very similar to that of the (Judicial) Commissioners in the Bill. Intelligence gathering measures can be implemented only when the Prime Minister or his or her designate gives a specific authorization. The Prime Minister's authorization is granted only after the Commission has given an opinion on the compatibility of the measure with the principles set forth in the law. The Commission's opinion is not binding on the Prime Minister. Nevertheless, if the Prime Minister decides to ignore the recommendation of the Commission, the Prime Minister must be prepared to explain his or her reasons. Moreover, the Commission can file an appeal with France's Supreme Administrative Court, the Conseil d'Etat, to challenge the Prime Minister's decision.

2.9 Like the US and the UK, France makes a distinction between internal and external surveillance measures. New, extended powers allowing the French State to carry out bulk interception of external communications were passed in earlier this year in the Loi du 30 Novembre 2015 relative aux mesures de surveillance des communications électroniques internationales (Law of 30 November relating to surveillance measures of international electronic communications). This allows for the interception and retention of both communications data and content upon an authorisation from the Prime Minister or his delegates. Unlike the interception provisions of the Law of 24 July, these authorisations are not subject to prior consultation with CNCTR. Both the Laws of 24 July and the Law of 30

November have been heavily criticised including a highly critical report from the United Nations Committee for Human Rights.

Following the November 13 attacks a number of additional measures have been proposed in France, including proposals that would allow the state to ban public Wi-Fi access in a state of emergency and access to the encrypted networks such as the Tor network at any time. There is at this juncture no clear direction from the French government as to how this could be enacted practically and there has been criticism of these developments.

Conclusions and Recommendations

2.10 The UK Parliament finds itself at a crossroads, as do governments in a number of nations. There is a balance to be struck between protecting citizens from the threats of terrorism and serious crime, but also the need for proportionality in the state's response. The threat of terrorism is real – as has been evidenced far too frequently of late, while the threat posed by organised crime is equally troubling. However, it is important not to confuse a security state with a safe state. No UK citizen would like to live under a system of mass surveillance and retention of personal data akin to the experience of citizens of East Germany. That was a security state not a secure state.

2.11 The UK Parliament is now tasked with the difficult job of ensuring state security while safeguarding the essential liberties of UK citizens. This briefing note outlines two opposing movements taken by comparable states recently. The Federal Government of the United States has chosen to rein in some of the more egregious activities of its national security agencies, to restate the rule of law and strengthen the role of an independent judiciary, and emphasise the protections of the Fourth Amendment. By taking bold decisions, such as the passing of the USA Freedom Act 2015, the public confidence and the capacity of the Federal Government in protecting both the liberties and safety of its citizens is enhanced. The French Government meanwhile seems to be in a purely reactive state. This may not be surprising given the terrorist actions at the Charlie Hebdo offices on 7 January 2015 and across Paris on 13 November 2015. A string of new laws have been passed and proposed which take less care of civil liberties. They centralise power in the office of the Prime Minister, fail to protect the role of the judiciary and the rule of law, and have been criticised extensively as being illiberal. These provisions have failed to make France or French citizens any safer. If we in the UK follow the French lead we will be no safer but we will lie in a less liberal state. In Benjamin Franklin's terms we will have given up essential liberty to purchase a little temporary safety. If we do this it may be argued we have changed our laws and our way of life in response to terrorist activity. This would be to do the terrorists' job for them, and it is why it is to be hoped that Parliament learns from and follows the American model and rejects the French model.

Part III: Bulk Personal Datasets in the draft Investigatory Powers Bill (Mr. Bernard Keenan)

3.1 The draft Investigatory Powers Bill is open about the need for the Security and Intelligence Services to generate and examine 'Bulk Personal Datasets' (BPDs) in order to obtain intelligence about threats to national security, prevent serious crime, and safeguard the economic well being of the UK. The avowal of the use of datasets relating to bulk

collection of many innocent people's information in modern intelligence work marks a significant change from the strict 'Neither Confirm Nor Deny' position that the Government adopted in response to legal challenges to the issue during hearings before the Investigatory Powers Tribunal in 2014.[590] The Bill is therefore a welcome change, not least because it is important that Parliament and the public are made aware of the nature of such data processing techniques and their implications for the rule of law. However, the Bill says very little about the nature of bulk data and how it is used. Furthermore, the Impact Assessment that has been published alongside the draft Bill makes clear that the Bill does not grant any new powers in relation to bulk data, it merely puts existing powers more explicitly into legislation and strengthens the oversight framework. This paper seeks to contextualise the use of BPDs in relation to how they can be used under the terms outlined in the Bill, and in terms of what they mean technologically.

3.2 Part 6 of the draft Investigatory Powers Bill (IP Bill) deals with Bulk warrants. Within Part 6, Chapter 1 contains provision for Bulk Interception Warrants, Chapter 2 relates to Bulk Acquisition Warrants, while Chapter 3 deals with Bulk Equipment Interference Warrants. These provide for the technical interception of content of communication, the acquisition of metadata about communication, and gaining unauthorised access to equipment in order to obtain such bulk information.

3.3 Part 7 of the IP Bill deals explicitly with the reality that this will interfere with personal information pertaining to innocent people. A BPD is defined at s. 150. It is a set of data that contains personal data about a number of individuals, the majority of whom are not and are unlikely to become of interest to the intelligence services, but which nonetheless the intelligence services have decided to retain for 'the purpose of the exercise of its functions'.

3.4 There are two types of BPD warrant outlined at s. 151(4). Subsection (a) provides for 'a class BPD warrant', which allows the Intelligence Services to obtain, retain or examine bulk personal datasets that fall within a 'class' described in the warrant, while s.151(4)(b) provides for "a specific BPD warrant" which authorises the production of a specific BPD described in the warrant.

3.5 Under s.153, class-based warrants are to be issued only where examination of that 'class' of data is deemed proportionate and necessary for operational purposes related to the three broad headings of national security, serious crime or the economic well-being of the UK related to national security. These are the three headings that underpin all authorisations that may be granted under the Bill. Under s.154, an intelligence service can apply for authorisation to produce and examine a dataset that is not covered by a broad class, or where it is considered appropriate to seek specific authorisation for a subject already contained within a given class of data.

Under Part 6 of the Bill, 'interception' of the content of communications pertaining to persons outside the UK can be freely collected and examined provided it is relevant to a specified topic specified in the warrant. Such interception data that pertains to persons present in the UK can only be *examined* if it is done explicitly for an Operational Purpose, but thereafter it is permitted. But the 'acquisition' of communications data is not subject to any

[590] Liberty & ors. V the Security Service, SIS, GCHQ IPT/13/77/H [2015]

territorial restrictions under Part 6. Communications data (or metadata) can therefore be gathered in bulk either from telecoms providers or by "any conduct which it is necessary to undertake in order to do what is expressly authorised or required by the warrant" (Section 122(7)(a)). If a communications provider cannot help, other technical means of obtaining data can be deployed.

3.6 In a sense, the introduction of BPDs warrants ties together the operational use of data already gathered under the various techniques authorised elsewhere in the IP Bill. While the Bill differentiates, for instance, between 'interception' of the content of communication, the 'acquisition' of 'communications data', and data obtained by equipment interference, these different sources of information all feed into the datasets that can be gathered and examined operationally under the heading of Bulk Personal Datasets. As the criteria for authorisation of a warrant under each heading are essentially the same, i.e. if it is necessary and proportionate to investigate a specific group or a general topic of interest, it is reasonable to assume that where a subject of concern is identified by the intelligence services, it can be examined and investigated by using BPDs. The proviso is of course that the investigation is deemed relevant to the interests of national security, prevention of serious crime, or safeguarding the economic interests of the country. These terms are ultimately defined by decision of the Secretary of State, with approval required from a Judicial Commissioner. Once authorisation is in place, the intelligence services are authorised to collect potentially massive sets of personal communications data from anyone, inside or outside the UK, which can be searched or sifted according to broad class-based criteria, or in some cases according to specific criteria. It is an extremely broad power.

Why bulk data?

3.7 What is Bulk Data and how is it used? For security reasons, it is impossible to know with any certainty what techniques are used within the intelligence services to analyse information. What follows is therefore to some extent speculative, although rooted in literature regarding the use of mass datasets in other areas of life that sufficiently indicates causes for concern.

3.8 Essentially, the analysis of any bulk dataset pertaining to a large group aims at uncovering patterns of behaviour that can allow the analyst to foresee make informed predictions about peoples' ideas and intentions before they materialise. It is by definition a speculative exercise, but one that is potentially capable of producing impressive results. The application of such so-called 'Big Data' techniques to commercial activities is growing all the time and attracting media attention.

3.9 In the situations envisioned by the IP Bill, the intelligence services are seeking to uncover useful intelligence information to inform predictions about future risk. The idea is similar to that in Philip K Dick's novel (and Tom Cruise film) *Minority Report*, where a predictive system aims at intercepting crimes before they are committed. The ambition is in guessing what is likely to happen and take action to change or prevent it, rather than waiting to investigate what has already happened. This is, in a sense, the whole purpose of state intelligence services.

3.10 A simple example is that of cross referencing a list of personal data of people with access to firearms against that of everyone suspected of wanting to illegally procure and use firearms. Many innocent people would thus be analysed, including their movements and transactions where they knowingly or unknowingly interact with suspects will be flagged up as a potential indicator of risk. Potential security threats are thus identified from subtle correlations identified across multiple datasets. This would be an example of a 'class-based' analysis drawing patterns from disparate sources of information.

Machine Learning and AI

3.11 Thanks to developments in computer software, mathematics and processing power, the tools used for analysing bulk datasets are evolving. From automatic trading software in the City to the trials of Google's self-driving cars, Artificial Intelligence (AI), 'machine-learning' processes are proliferating. Broadly speaking this refers to computer systems that have the capacity to refine their own predictive algorithms based on further experience. As with a human child learning to interact with the world, the program makes links between data, establishes a model that would have predicted that data, and then tests that model against further data as it becomes available. The further experience can confirm the initial model or refute it, but either way the machine learns to refine its model. The program uses each new 'experience' to refine its model of reality so that its subsequent predictions become a little more accurate.

3.12 Such artificially intelligent programs are thus capable of constantly changing and constantly refining the parameters of its predictions. Logically, the more information that becomes available for analysis, the better the predictive capacity of AI. At the same time, the more information that is available, the more that human operators rely on Artificial Intelligence to sift through it to find meaningful links. Thus the analysis of large sets of data by machine promises huge efficiency and ever-growing accuracy. Under a Bulk Personal Dataset warrant, the agencies would be able to produce large sets of personal data according to themes that are of interest, and analyse them for patterns to apply in the future.

Concerns

3.13 The concern with the use of such analytic processes is not straightforwardly about privacy in the classic sense. When we think of surveillance powers in the classic sense, we worry about the private contents of one's letters being uncovered – our personal thoughts, private embarrassments, political opinions, medical conditions, financial records, business plans, and so on. Both democracies and totalitarian states have found reasons to secretly investigate the private communications of citizens at different points in history.

3.14 Analysis of Bulk Personal Datasets includes these concerns to some extent, but it goes beyond them. The processes are arguably less intrusive into personal privacy, in that the complete details of an innocent individual's life are not usually of interest and the only thing 'reading' an innocent person's information is a disinterested computer. The algorithm's interest is in how a particular set of attributes is related to a particular set of outcomes.

3.15 On the other hand, the decisions and risk factors produced by analysis of Bulk Personal Datasets threaten personal autonomy and risk producing systemic discrimination, stereotyping, and biased decisions, both at the policy level and operational level. First, it is clear that a massive amount of personal information pertaining to innocent persons will be collected and 'crunched' by analysts. The potential for abusing such a large collection of data is vast and it is vital that data is used strictly for authorised purposes and erased after its operational relevance has ended. Under the current draft, information will only be erased once it is no longer 'likely' to be of use for the purposes of a warrant. Given that the analysis of BPDs is essentially speculative, this is arguably too low a threshold for authorising long-term retention of an individual's data in a BPD.

3.16 Second, personal autonomy is affected. Individuals at home in the UK or abroad will have no control over the type of processing of their personal information that the agencies carry out for authorized purposes. This may lead to operational or policy decisions that profoundly affect that individual without their knowledge or consent. Decisions may be taken based on correlations identified in Bulk Personal Datasets, but correlation is not causation. Risk factors based on correlations do not offer any causal explanation as to *why* an individual or group are deemed to be a risk. The only certainty is that a computer has observed a pattern. The difficulty then is that an analyst presented with such a decision is incapable of independently evaluating the quality of the decision, as they cannot know clearly why it has been reached.[591] The inability to offer a substantive rational reason for a decision undermines the legal premises upon which accountability in government is based.

3.17 This in turn raises the problem of due process. Data analytics is not a neutral process. Before a dataset can be analysed for patterns, an analyst must define the terms of interest. How these terms are defined has a huge impact on the results observed. [592] Yet the intelligence services necessarily operate in secrecy. Non-transparency means that where innocent people may be flagged up for attention, such as further surveillance or equipment interference, they will not be able to seek redress unless the IPC is able to investigate and inform them after the fact. Furthermore, the public will not be able to assess the success or failure of such analyses in protecting security unless these techniques are explicitly and transparently described in the public reports of the IPC.

3.18 Finally, 'mission creep' is a real concern. As explained above, the point of gathering and analysing bulk data is to identify hitherto unknown patterns. By nature, it is a speculative exercise. The temptation then is towards 'total' interception of data in order to meet the lawful objective, as all data is *potentially* useful. Thus General Keith Alexander's alleged instruction to the NSA to 'collect it all'.[593] This question increases the pressure for effective oversight, transparency, and accountability.

---

[591] Van Otterlo, 'A Machine Learning view on Profiling', in Hildebrandt & de Vrijes (eds.), *Privacy, Due Process and the Computational Turn* (2013)

[592] Van Otterlo, 'A Machine Learning view on Profiling', in Hildebrandt & de Vrijes (eds.), *Privacy, Due Process and the Computational Turn* (2013)

[593] 'For NSA chief, terrorist threat drives passion to 'collect it all', Ellen Nakashima and Joby Warrick, *Washington Post,* 14 July 2013, https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html, accessed 16 November 2015.

Oversight and Transparency

3.19 In the long run, the Impact Assessment suggests, the public are otherwise likely to become concerned about the use of BPDs, the content of which is mostly comprised of data concerning individuals who are of no operational interest to the Services. The Impact Assessment also states that specific training in understanding the use of BPDs will be provided to the Judicial Commissioners tasked with oversight.

3.20 The intelligence services must work in secrecy, and cannot reveal the methods applied to either the gathering of data or its analysis. Hence the public will not be in a position to evaluate the successes or failures of such decision-making processes. Transparency must be carefully considered in this context. The information processes involved in analysing bulk data are not fixed in their uses. They are potentially useful and, despite the allusion to the film *Minority Report*, the dystopian future that they conjure up is far from an inevitable outcome. But how to mediate a transparent and accountable system for the implementation of such vast data processing surveillance system is crucial.

Part IV: Beyond privacy: the data protection implications of the IP Bill (Dr. Orla Lynskey)

How will the proposed IP bill influence digital communication? What will the implications be for the security of our data? This section of the brief looks at the EU law context of new surveillance mechanisms, and explains the difficult technological, economic and fundamental right implications of the policy choices.

4.1 In an era of digital communications, personal data flows do not respect national borders. UK residents communicate with friends and family living outside the UK's borders while internet communications are routed all over the world when making their way from our computers and other connected devices to their final destination. At the same time, there is increasing public awareness of the dangers caused by mass data collection and data profiling. The Talk Talk and Ashley Madison data breaches, the Snowden revelations, the suspension of Safe Harbor data transfers between the EU and the US and the (misnamed) 'Right to be Forgotten' judgment by the EU Court of Justice (CJEU) have all made news headlines in recent years, and stakeholders – activists, businesses, policy-makers, the judiciary – are increasingly aware of the need to take personal data protection seriously.

4.2 This dual dynamic – the global nature of digital information flows and the increased awareness of data protection and privacy – poses a challenge for national lawmakers. Any law introduced influencing the flow of information, such as the proposed Investigatory Powers Bill (IP Bill), will have effects in other countries beyond the UK, and will influence where companies choose to invest and to develop their operations. This Briefing Paper will therefore put the IP Bill in its EU law context. It suggests that, beyond privacy, the IP Bill will jeopardise two aspects of the right to data protection: individual autonomy and personal data security. In addition to these rights implications, the IP Bill may also have economic implications by discouraging technology industry investment in the UK.

The right to data protection: A 21st century right for a 21st century phenomenon

4.3 While historically there has been no right to privacy recognized by the common law in the UK, such a right has been developed through the case law of the Courts. This has been done by expansively interpreting existing legal concepts, such as 'breach of confidence' and 'misuse of private information', in light of the Article 8 ECHR right to private life and privacy of correspondence. Individuals who believe the government, or other public bodies, have interfered with their right to privacy can now rely directly on Article 8 ECHR before UK Courts.

4.4 The EU Charter of Fundamental Rights (EUCFR), binding on Member States when 'implementing EU law' since 2009, contains both a right to privacy (Article 7) and a right to data protection (Article 8). While initially courts in the UK treated data protection as a subset of the right to privacy with no independent legal value, the UK courts now recognize that these rights are distinct. Most recently, the Court of Appeal suggested that the right to data protection is more specific than the right to privacy, is not limited in its meaning and scope by the right to privacy and that it has no counterpart in the European Convention of Human Rights (ECHR). We must therefore consider whether the IP Bill would withstand scrutiny under this independent right to data protection.

4.5 The right to data protection is a 21st century right for a 21st century phenomenon: the exponential increase in scale of automated processing of personal information. The added value of this right is that that in addition to protecting 'private' information, it includes within its scope our publicly available information. It also gives individuals certain rights over this information that are not traditionally associated with privacy, such as a right to delete it in certain circumstances and the right to obtain this information in a portable format to encourage switching between providers. In this way, it is suggested that the right to data protection gives individuals more control over more personal data when compared to the right to privacy. This individual control over personal information is not absolute and it gives way in certain circumstances to protect other rights, such as freedom of expression, and other interests, such as national security. Nevertheless, the enhanced control over personal information given to individuals by the right to data protection acts as a counter-balance to the power and information asymmetries that persist between individuals and the public and private entities that benefits from processing their data. In theory, the right to data protection also enhances the negative freedom of individuals: that is, the freedom of individuals to act in an autonomous way without impediments or obstacles. It does this by ensuring that individuals have information regarding how and why their personal data are processed so that they can accurately estimate what future implications this data processing will have for them.

4.6 The provisions of the IP Bill facilitating access to so-called 'bulk personal datasets' curtail these benefits of the right to data protection. The IP Bill foresees that bulk datasets held by public and private organisations can be accessed by Security and Intelligence Agencies (SIAs). The IP Bill distinguishes between 'specific' bulk datasets and 'class' bulk datasets. A specific bulk dataset might, for instance, be the National Insurance Number database while a class bulk dataset might be all information held by football clubs about their season ticketholders

or CCTV data held by local borough councils. However, the dividing line between these two categories is not clear-cut, and it is possible that class bulk dataset collection could be defined broadly to enable mass data profiling. For example, one class of dataset might be all property registration and rental information of Londoners. While a warrant, valid for up to 6 months, must be sought for use of these bulk datasets pursuant to the so-called double-lock procedure, such bulk data profiling can have several pernicious effects.

4.7 The potential pitfalls of using automated 'machine-learning' processes on bulk data are clearly set out in the Briefing Paper on Bulk Personal Datasets in the draft IP Bill. Suffice to recall here that the concerns identified therein – in particular, that such datasets may be abused if adequate safeguards are not in place and, that decisions based on processing such datasets may profoundly affect individuals without their knowledge or consent – are concerns which fall within the scope of the right to data protection. By facilitating profiling and discrimination between and within classes of individuals without a 'lead', the spirit of the IP Bill is antithetical to that of the right to data protection: it conflicts with the autonomy and personality-enhancing aspects of the right to data protection. It also sits uneasily alongside other more-established rights such as the presumption of innocence and freedom from discrimination. An individual who is singled out from others simply because he is part of a particular group and has particular characteristics or interests that correlate to 'suspects' or persons of interest to the SIAs cannot have negative freedom. He may not know that he is part of this group, or why this group is set apart from others, and he also may not know what future impact this may have on him. This Kafkaesque scenario shall become a reality for some UK residents under the IP Bill.

Data security as a facet of the right to data protection

4.8 The right to data protection also protects data security. Indeed, data security is described as the 'essence' of the right to data protection in the judgment of the CJEU in *Digital Rights Ireland*. It would therefore appear that to comply with the right to data protection, data processing operations – such as those envisaged by the IP Bill – must have technical and organizational measures in place to tackle the destruction, loss or alteration of data. Moreover, in *Digital Rights Ireland* the ECJ noted with disapproval that providers subject to data retention obligations could have regard to economic considerations when determining the technical and organizational means to secure the personal data retained. This suggests that the level of data security required is a stringent one.

4.9 At present in the UK, SIAs rely on a 1994 Act to hack equipment including computers, laptops and mobile devices. The IP Bill provisions dealing with 'Equipment Interference' provide a more explicit legal basis for this hacking. These provisions are unlikely to comply with the data security requirement of the right to data protection. In his Report, David Anderson QC, the Independent Reviewer of Terrorism Legislation, noted that there was a 'dizzying array of possibilities' open to SIAs to engage in equipment interference with some being so intrusive that they could rarely be legal.

4.10 Two aspects of 'equipment interference' merit particular attention. First, communications service providers will be subject to an explicit obligation to assist in giving effect to equipment interference warrants served by SIAs. This has raised alarm bells for

industry representatives and technology experts who argue that by creating technological backdoors to facilitate such interference, all information systems will become more vulnerable. Who can guarantee that a backdoor, created for SIAs, will not itself become an easy target for those terrorists and thieves whom this legislation is designed to target? Secondly, the IP Bill facilitates bulk equipment interference with the devices of individuals outside the UK by the SIAs for the purpose of domestic national security. Would we allow the German government to hack the mobile phones of vast swathes of the UK population who are not suspected of criminal or terrorist activity? If not, can such extraterritorial principles be legitimately imposed on the residents of other countries? Would this be in line with the UK government's international obligations, in particular its ECHR obligations? Such questions remain to be answered.

Influence of EU Law on Domestic Data Retention Legislation

4.11 Will the EU right to data protection have an impact on the IP Bill? The short reply is that as the IP Bill is domestic legislation it is not subject to the EUCFR, and thus the Article 8 right to data protection. Indeed, the EU has no general competence to legislate in the field of fundamental rights and, although Member States must respect general principles of EU law and the EUCFR, they must only do so when they are 'implementing EU law'. This begs the question of whether the UK is 'implementing EU law' if it adopts the IP Bill. While the intuitive answer to this may be a definitive no, the legal reality is more complex. The term 'implementing EU law' has been interpreted expansively by the CJEU in *Pfleger* to include situations where a Member State seeks to rely on a derogation from EU law. Article 5 of the EU's E-Privacy Directive sets out a general principle of confidentiality of communications and related traffic data. Article 15(1) of that Directive allows Member States to adopt legislation to restrict the scope of such rights when necessary for, amongst other things, state security. It specifically allows Member States to 'adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph'. Thus, data retention legislation such as the IP Bill is based on a derogation provided for by EU law and is 'implementing EU law', it must therefore respect the EUCFR.

4.12 The CJEU has had the opportunity to assess the compatibility of EU data retention legislation with the EUCFR rights to data protection and privacy in *Digital Rights Ireland*. In its judgment, the CJEU declared the Directive to be void, as it constituted a wide-ranging and particularly serious interference with those rights. The interference could not be justified as it went beyond what was necessary to achieve its stated aims. Indeed, the Court identified an extensive catalogue of shortcomings of the Directive. Following the judgment of the Court in *Digital Rights Ireland*, the UK was concerned that the legal basis for its existing data retention legislation was in doubt and it enacted new legislation (the Data Retention and Investigatory Powers Act (DRIPA) 2014). This legislation, which will expire at the end of 2016, was challenged before the High Court on the grounds that it was incompatible with the findings in *Digital Rights Ireland*. The High Court agreed, albeit on the basis of a very narrow interpretation of the ECJ's judgment. The High Court finding was then appealed to the Court of Appeal, which has stayed the proceedings in order to refer a number of questions to the ECJ. In particular, the Court of Appeal wishes to ascertain whether – contrary to the findings of the High Court – the shortcomings of the Directive highlighted by the ECJ in its judgment

constitute mandatory requirements which national legislation must respect. The answer to this question will be critical to the validity of the IP Bill.

4.13 It could be argued that only rules applicable to data *retention* fall within the scope of EU law, with rules relating to *access* by government security agencies falling outside the scope of EU law. This neat distinction is blurred by the close links between retention and access. Indeed, it has been observed that the lawfulness of collection and retention cannot be accessed without considering how access and use is regulated. This also follows from *Digital Rights Ireland* where the Court reasoned that the retention of data was a prima facie interference with rights, which could have been justified only if adequate safeguards had been in place governing access and use. An attempt to limit the application of the EUCFR right to data protection by distinguishing between the 'retention' provisions in the IP Bill (where it would apply), and the 'access' provisions (where it would not) will therefore be a difficult and somewhat artificial exercise. It may however be easier to carve the 'equipment interference' provisions out from the EUCFR's reach as they are more closely related to domestic hacking rules (such as the Computer Misuse Act 1990) than the EU's (void) Data Retention Directive. However, it is suggested that even if not obliged by EU law to respect the rights to data protection and privacy, it may be in the economic interest of the UK to do so.

Splendid isolation? The Potential Economic Implications of the IP Bill

4.14 Enthusiasm, at least judicial enthusiasm, for blanket data retention legislation has been waning across EU Member States even before the *Digital Rights Ireland* judgment. Prior to that judgment, domestic data retention legislation was successfully challenged in Bulgaria, Romania, Germany, the Czech Republic, and Cyprus in addition to the challenges in Ireland and Austria, which led to the judgment. Since the CJEU's findings, constitutional courts in Austria, Slovenia, Belgium, Romania and Slovakia as well as a district court in the Netherlands have found national data retention to be incompatible with the judgment and thus invalid. As has been documented in another Briefing Paper, the introduction of the Freedom Act 2015 in the USA also marks a move away from this model. The UK may soon find itself in an isolated position.

4.15 From a legal perspective, this isolation would be problematic in the event of a 'Brexit'. The CJEU suspended safe-harbor data flows between the EU and the US as the US did not offer the data of EU residents an 'adequate' level of personal data protection. This finding was admittedly a controversial one. Nevertheless, at present the UK is benefitting, as an EU Member State, from a presumption of adequacy regarding its personal data processing. Should the UK leave the EU, the EU may refuse to recognize the safeguards for access to personal data pursuant to the IP Bill in the UK as 'adequate'. This would seriously hamper data flows between the UK and other EU Member States.

4.16 A second more predictable implication is that if the UK is one of few EU Member States which obliges communications service providers to facilitate equipment interference, companies will move their manufacturing and technological operations elsewhere. Trust is a key component of success in the digital environment. If this trust in UK communications systems is undermined by the spectre of equipment interference and data security concerns,

industry might relocate to countries, which are more respectful of data security issues. Encryption techniques are of no value once a network or device is hacked as data is ordinarily unencrypted once it is stored on a machine, system or network. Thus, even the most informed and engaged individuals will not be able to secure their data and their autonomy under the system as envisaged. What is bad for fundamental rights will ultimately become bad for business.

4.17 The IP Bill must be put in its international context. The provisions of the Bill which facilitate equipment interference and the use of bulk personal datasets are out of line with the spirit and the letter of the EU's right to data protection. Moreover, by compelling communications service providers to assist Security and Intelligence agencies in their task, the security of our data is undermined.

Biographies of Authors.

Mr. Bernard Keenan is a PhD candidate at the London School of Economics, where he obtained his LL.M in 2008. He researches the use of classified material in legal proceedings in the UK. Before beginning his PhD in 2013, he worked as an immigration lawyer for five years, qualifying as a solicitor.

Dr. Orla Lynskey is an Assistant Professor of Law at the London School of Economics where she teaches courses on Cyberlaw, EU Law and Digital Rights. Her research is in the field of technology regulation, with a particular interest in EU data protection law and intermediary/platform power. Her most recent work includes a monograph on *The Foundations of EU Data Protection Law,* published by Oxford University Press. Prior to entering academia, Orla worked in Competition law practice in Brussels and as an academic assistant at the College of Europe, Bruges.

Professor Andrew Murray is a Professor of Law at the London School of Economics where he researches and teaches in the fields of Internet and new media law, including the laws of digital surveillance and digital privacy. He is author/editor of a number of books including Human Rights in the Digital Age (2005), The Regulation of Cyberspace (2007) and Information Technology Law: The Law and Society (2013) as well as the author or co-author of over thirty academic journal papers. He was in spring 2015 a visiting Professor at the Institut d'études politiques de Paris (Sciences Po) and is from 2014-2020 a visiting Professor at the Vrije Universiteit Amsterdam (Free University, Amsterdam).

21 December 2015

Eric King—written evidence (IPB0106)

The ability to live a private life is a human right and public good that enables our society and our democracy to function. Increasingly, that private life, including a person's most intimate moments, is experienced, in one form or another, in the digital world.

As a result of advancements in technology, in recent years, Britain's security and intelligence agencies' capability to acquire, process, and analyse information about a person's private life, at scale, has dramatically expanded.

Upholding privacy necessarily requires that surveillance must be restricted to only that which is strictly necessary and proportionate. Societies around the world have benefited greatly from technological constraints that have historically kept the more extreme ambitions of intelligence agencies in check; protecting that ability to live a private life. Yet, slowly but surely, those technological constraints are being lifted.

The question I invite the committee to consider, is not what *can* be done in the field of surveillance, given the available technology, or what the previous practice has been of our intelligence agencies, but, rather, what *should* now be done. Now that our society can no longer rely on technological constraints to protect us against unnecessary intrusions into our private communications, it is critical that legislation exists to guard against such unnecessary intrusions. It is my view that there has never been a more important moment to set strong limits, in both law and policy, on our intelligence agencies' capabiltiies, to ensure they are only used where necessary and proportionate.

Executive Summary:

Due to the short timeframe given to prepare evidence, and the length and complexity of the draft Bill, I regret I am unable to provide detailed comments on all issues. Instead, I have elected to provide the Committee with a factual background and high level recommendations on the "bulk" powers contained in the Bill, to inform the Committee's consideration of how the powers in the draft Investigatory Powers Bill will be put to use in practice.

The majority of powers contained in the Bill, including the most intrusive, have not been considered by Parliament before. Operational cases have not been made for the majority of these powers. It is essential that such operational cases are presented so as to allow this Committee, Parliament, and the public to properly scrutinise the necessity, proportionality and likely effectiveness of the powers.

The use of Bulk Interception to collect ~50 billion internet communications a day, from more than a quarter of all undersea cables coming in and out of the United Kingdom, in order to create "a web browsing profile for every visible user on the Internet" and subject those emails, videos, messages, and web searches to automated analysis for target development, is not a proportionate interference with civil liberties.

The use of Equipment Interference to "exploit any phone anywhere, anytime" including targeting people "not of intelligence interest" is dangerous, and illiberal. The methods employed to undertake Bulk Equipment Interference with respect to equipment maintained by companies, and individuals who are not themselves national security threats and who are not suspected of any criminal wrong doing on an "industrial scale" is counter-productive to cyber security goals.

Powers such as Bulk Communications Data Acquisition are not only disproportionate, they are ineffective; such a conclusion has already been reached in the United States, where bulk communications data acquisition programmes have been ended after two government reports concluded they were ineffective, while concurrently criticising the disproportionately intrusive nature of the power.

There is a paucity of information surrounding Bulk Personal Datasets, making it difficult to assess the scope of the power. They should be approached with great caution, as Bulk Personal Datasets may end up being the most intrusive and least-regulated power proposed in this draft Bill.

New powers and the lack of operational cases

The committee should not consider the majority of the powers in this draft Bill to be pre-existing. While almost all of the capabilities are currently in use by our intelligence agencies, they were authorised under secret interpretations of law, that Parliament had not consented to, nor were aware of, and their lawfulness is currently being considered by the Investigatory Powers Tribunal, the European Court of Human Rights and the Court of Justice of the European Union .

It was not until the February 2015 publication of the Equipment Interference Code of Practice[594] that computer hacking, or what the agencies internally call Computer Network Expoitation (CNE) became avowed. At the time of drafting, GCHQ maintains, in respect of ongoing litigation in the Investigatory Powers Tribunal, that Bulk Equipment Interference has still not been avowed.

It was not until the March 2015 publication of the Intelligence and Security Committee's (ISC) report[595] that Bulk Interception, including that of large international undersea cables, was avowed. This is despite litigation having been conducted in the Investigatory Powers Tribunal for the preceding two years in which GCHQ invoked a Neither Confirm Nor Deny stance with respect to the existence of Bulk Interception capabilities.

It was not until the March 2015 publication of the Intelligence and Security Committee's report[596] earlier this year that Bulk Personal Datasets was avowed. As the ISC stated "*…until publication of this Report, the capacity was not publicly*

[594] United Kingdom, Home Office (6 February 2015) Equipment Interference Code of Practice. [Online]. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/401863/Draft_Equipment_Interference_Code_of_Practice.pdf [Accessed 28 September 2015]

[595] Privacy and Security: A modern and transparent legal framework, Intelligence and Security Committee.

[596] Privacy and Security: A modern and transparent legal framework, Intelligence and Security Committee.

acknowledged, and there had been no public or parliamentary consideration of the related privacy considerations and safeguards"

It was not until November 2015 that the Home Secretary herself avowed[597] the fact that MI5 had been using an obscure statutory provision contained within Telecommunications Act 1984 to collect domestic phone records in bulk and subject them to data mining, something that Government intends to continue pursuant to the draft Bill's provisions on Bulk Acquisition Powers and Bulk Personal Datasets.

Prior to those avowals, there was no official suggestion - either from Government, the agencies themselves or intelligence oversight bodies - that such activities were being undertaken. Indeed, efforts of some oversight bodies[598] to inform the public further were frustrated by the agencies' insistence in keeping the capabilities secret.

Any suggestion that such secrecy was justified on the basis of an overriding need to obscure the capabilities of the security agencies from those who might potentially be subject to such capabilities, in order to prevent the circumvention or avoidance of surveillance, is clearly refuted by the inclusion, in great detail, of such powers in the present draft Bill.

Due to the lack of avowals and the obfuscated language of existing legal frameworks, no piece of legislation expressly references any of the above capabilities with sufficient clarity for them to be have appropriately considered by Parliament. As such it is not until this draft Bill that Parliament has ever been given the opportunity to debate the necessity of, or the operational case for, many of the most intrusive powers in this Bill.

Perhaps what is most striking about the fact is the clear absence of any operational case for the majority of the powers in this Bill. This absence is particularly peculiar given that the operational case, if there were to be one, should have been relatively easy to put together. This is because many of the most intrusive capabilities are already in use by the agencies and have been for a long time, regardless of the non-existence of strong statutory footing.

As a result, there should be more than a decade's worth of practice to draw from to show the effectiveness of such capabilities, to highlight examples of successes of some powers and failures of others, and provide analysis of the unique impact certain programmes and techniques have had.

Perhaps one reason why there is such a lack of an operational case being made is that, despite the extraordinary scale of intrusion, the agencies cannot prove that bulk powers have had a discernible impact.

---

[597] Gordon Corera, "MI5 'secretly collected phone data' for decade," *BBC News*, available at: http://www.bbc.co.uk/news/uk-politics-34729139

[598] The efforts of Interception of Communications Commissioner's Office to improve transparency and public engagement in particular should be noted in this regard.

Conclusion and recommendation

Operational cases should be publicly made for all bulk powers contained in the draft Bill to allow Parliament and the public to properly scrutinise the necessity, proportionality and likely effectiveness of the powers.

Bulk Interception

Although Britain has a long history of gaining access to communications via the interception of undersea cables, the volume of communications that is being intercepted and analysed under TEMPORA is orders of magnitude greater, and as a result, entirely different, from anything undertaken in GCHQ's history.

Despite statements by the Home Secretary in 2008 explaining that the Government had "no plans for an enormous database which will contain the content of your emails, the texts that you send or the chats you have on the phone or online,"[599] it is now known that such a database had indeed been built, and was growing daily.

Two years earlier, in 2007, a process of modernisation had taken place at GCHQ resulting in a twenty-fold increase in GCHQ's capability[600]. More than 50 billion pieces of internet and phone content were being intercepted, processed and analysed every day. An enormous database with the content of emails, texts, and telephone calls did indeed exist. By 2009 GCHQ's access to undersea cables had increased by a further 7000%.

I have summarised the rapid expansion of GCHQ's Bulk Interception capacity in **Annex A**.

Today, this un-targeted collection is used to drive different programmes to achieve extraordinary levels of intrusion at a previously unimaginable scale.

One programme, KARMA POLICE, used the communications captured in bulk to provide the agency with "a web browsing profile for every visible user on the Internet."[601] This is not mere passive collection and storage of private communications, but an active attempt to build detailed profiles, akin to a physical dossier or file on everyone on the internet, based on individuals' web searches and browsing history. As extraordinary as it sounds, nevertheless, this was the stated goal of the GCHQ programme.

The volume of data collected is enormous and so most of the material cannot be reviewed by a person. At such a scale, it is impossible to immediately determine what will be of interest to GCHQ, nor is it possible to immediately filter out the private communications of perfectly innocent people who are not suspected of anything. Instead, GCHQ treats every piece of information intercepted as potentially suspicious, pieces it back together, and subjects it to intrusive processing, filtering, and analysis. GCHQ then mines the data for correlations and patterns, suspicious words or phrases, relationships or connections using powerful computers, building profiles on people automatically.

In this way, the private communications of everyone who is caught up in this net are the subject of experimentation in an attempt to determine how suspicious a certain person, about whom nothing previous was known, may or may not be. Emails between close friends,

---

[599] Giant database plan 'Orwellian', BBC News, available at: http://news.bbc.co.uk/1/hi/uk_politics/7671046.stm

[600] Intelligence and Security Committee, Annual Report 2006–2007

[601] Ryan Gallagher, "PROFILED From Radio to Porn, British Spies Track Web Users' Online Identities", *The Intercept*, available at: https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities/

phone calls between family members, internet searches about medical conditions, and the browsing of news websites for political views will all be examined and graded.

It is no surprise that this has happened. Indeed, it is a predictable consequence of an agency with an engineering mindset, focussed on an important mission, and pushing the limits of what is possible, in secret. However, collection at this scale cannot be justified.

Technological limits, and financial constraints were previously keeping the agencies in check; today, they simply do not exist. With more funds being made available, and technology obliterating obstacles to surveillance, we must look to law to place limits. Regrettably, this draft Bill places no meaningful constraints on this capability. Instead, it provides GCHQ with the renewed mandate to scale even further, expanding its collection and analysis to new highs.

While in 2009, a quarter of all undersea cables that land in the United Kingdom were being analysed by GCHQ, as the technology becomes more affordable, that proportion will only increase. GCHQ already has plans to grow TEMPORA capabilities at multiple processing centres based within the UK and overseas.[602]

This draft Bill must set hard limits to constrain that practice, and to ensure only that which is necessary and proportionate is undertaken.

Conclusion and recommendations

Due to historic secrecy around the capability, the operational case for why Bulk Interception powers are necessary has never been made. In my view, given the extraordinary reach and depth of intrusion into innocent people's private communications, and the striking absence of a detailed operational case, Bulk Interception capabilities in the form they are currently used are not a proportionate activity and should be prohibited.

Although I make the above recommendation in the strongest terms, if Bulk Interception powers are retained in the draft Bill, the following minimum safeguards must be introduced into the legislation:

> **Only the targeting of communications relating to specific identifiable targets, using 'hard selectors' should be permitted. The use of 'soft selectors' or 'about' selectors should be prohibited.**
>
> **The use of Bulk Interception for the purpose of target development, or to "search for traces of activity by individuals who may not yet be known to the agencies" should be prohibited.**
>
> > **The automatic creation of detailed profiles tying communications captured in Bulk to individuals not considered a national security threat, or suspected of any crime should be prohibited.**
> >
> > **A policy must be published that sets out a procedure for determining bearer selection.**

[602] GCHQ Wiki entry on TEMPORA, *Der Spiegel*, available at http://www.spiegel.de/media/media-34103.pdf

Bulk Equipment Interference

Bulk Equipment Interference is a newly coined term pertaining to a wide range of capabilities including what the Agencies call Computer Network Exploitation (CNE), but which is more commonly known as hacking. CNE is the most intrusive and dangerous capability the Agencies possess.

At **Annex B,** I provide detail about the scale of the deployment of CNE capabilities, their unintended consequences and further recommendations.

GCHQ regularly hacks companies who are not themselves threats to national security, nor suspected of involvement of any wrongdoing. They did so with respect to Belgium's largest telecommunications provider, Belgacom, incurring the company £12 million[603] in clean up costs, with the aim of using Belgacom as a launch pad for further attacks. GCHQ hacked into the internal computer network of Dutch SIM-card company Gemalto, stealing encryption keys used to protect the privacy of cellphone communications across the globe. A plethora of German companies including Deutsche Telekom AG[604], Netcologne, Stellar, Cetel, and IABG[605] have all been targeted by GCHQ in recent years.

The agencies do this to help enable other missions, and future attacks; attacking these companies is merely a means to an end. In my opinion, attacking these companies is neither necessary nor proportionate. Britain should be working with its allies, not attacking them. Undertaking these activities only encourages a race to the bottom, and places British companies at greater risk. There is nothing in the draft Bill that would limit the scope or scale of these attacks.

Unintended consequences are common. Whole countries communications infrastructure have been accidentally taken-off line by CNE operation gone wrong. Even malware used in highly targeted attacks, such as those used in Stuxnet targeting Iranian nuclear facilities, inadvertently spread, and are still being found damaging corporate networks.

Worse still, to undertake these attacks, agencies exploit, or implant security vulnerabilities in technology. By stockpiling these vulnerabilities and using them offensively as part of attacks, GCHQ are preventing preventing potentially millions of individuals and companies from being protected.

Rather than these being used in a targeted manner, only in extremis, GCHQ intend to deploy this capability in bulk. This is improper and reckless.

---

[603] Doug Drinkwater, Belgacom says alleged GCHQ APT attack cost firm £12 million, *SC Magazine*, available at: http://www.scmagazineuk.com/belgacom-says-alleged-gchq-apt-attack-cost-firm-12-million/article/378870/

[604] Grothoff, C. et al (14 September 2014) Map of the Stars: The NSA and GCHQ Campaign Against German Satellite Companies, *The Intercept* [Online]. Available from: https://firstlook.org/theintercept/2014/09/14/nsa-stellar/ [Accessed 1 October 2015]

[605] Grothoff, C. et al (14 September 2014) Map of the Stars: The NSA and GCHQ Campaign Against German Satellite Companies, *The Intercept* [Online]. Available from: https://firstlook.org/theintercept/2014/09/14/nsa-stellar/ [Accessed 1 October 2015]

Conclusion and recommendations

No detailed operational case has been made for these powers, nor is there any publicly available analysis of the implications or risks of deploying Equipment Interference with respect to a range of factors, including for the UK's cyber security. It is my view that the the use of Bulk Equipment Interference should be prohibited.

Although I make the above recommendation in the strongest terms, if Equipment Interference powers are retained in the draft Bill, the following minimum safeguards must be introduced into the legislation:

The UK government should fully support and not undermine cyber-security efforts, including not in any way subverting, undermining, weakening, making or keeping vulnerable generally available software and hardware.

The targeting of companies or "individuals who are not intelligence targets in their own right" and thus not a threat to national security, or not suspected of any criminal wrongdoing, should be prohibited.

An equities policy must be published that sets out a procedure for determining whether flaws or vulnerabilities discovered or purchased by the government should be disclosed to the public or other relevant actors.

Government agencies engaged in CNE operations should be prohibited from impersonating trusted professions, including doctors, lawyers, and journalists. They should also be prohibited from deploying CNE in such a manner that impersonates critical cybersecurity infrastructure such as those used by software companies to deliver security updates.

Companies should not be compelled, required, or pressured to assist with the development or deployment of CNE.

Where CNE has been used against devices owned by individuals who are subsequently criminally prosecuted, there should be a obligation to notify the individual, and provide complete details of how CNE was used to ensure a fair trial.

Bulk Communications Data Acquisition

The use of Bulk Communications Data Acquisition to collect domestic phone records in bulk and subject them to data mining has until recently been kept secret. Nick Clegg MP stated that even inside Government "*only a tiny handful of senior cabinet ministers*" knew of such a practice.[606] The Home Secretary only avowed[607] to Parliament the fact that MI5 were relying on an obscure statutory provision contained within Telecommunications Act 1984 in November 2015. When announced, David Anderson QC told the BBC that the "*law was so*

[606] Patrick Wintour, Only 'tiny handful' of ministers knew of mass surveillance, Clegg reveals, *The Guardian*, available at: http://www.theguardian.com/world/2015/nov/05/nick-clegg-cabinet-mass-surveillance-british-spying

[607] Gordon Corera, "MI5 'secretly collected phone data' for decade," *BBC News*, available at: http://www.bbc.co.uk/news/uk-politics-34729139

broad and the information was so slight that nobody knew it was happening". He added it was "*so vague that anything could be done under it.*"[608]

I explain what is known about Bulk Communications Data Acquisition at **Annex C**.

In the United States, a similar power has previously existed under Section 215 of the USA PATRIOT Act. After the use of what in the US is called the "bulk telephone records programme" was revealed b Edward Snowden, two independent bodies undertook reviews of, inter alia, the use of this power, in order to determine in part whether the operational case studies put forward by the US government to justify the programme were credible and accurate.

With access to classified material, the The President's Review Group on Intelligence and Communications Technologies concluded: "*Our review suggests that the information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders*".[609]

Similarly the Privacy and Civil Liberties Oversight Board concluded in the same manner that "*we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of an attack*."[610]

Less than a month ago the US ended the Section 215 bulk phone records program.

Given that two independent bodies, both of which had access to classified material, found a directly similar power ineffective and disproportionate, it should be concluded that the Government's Bulk Communications Data Acquisition powers are equally ineffective and disproportionate too.

Conclusion and recommendations

Bulk Communications Data Acquisition powers should be rejected on the grounds that they are ineffective and overly intrusive, until such a time that an operational case to rebut that presumption is made, and can be adequately scrutinised.

Although I make the above recommendation in the strongest terms, if Bulk Communications Data Acquisition powers are retained in the draft Bill, the following minimum safeguards must be introduced into the legislation:

[608] Gordon Corera, "MI5 'secretly collected phone data' for decade," *BBC News*, available at: http://www.bbc.co.uk/news/uk-politics-34729139

[609] Liberty and Security in a Changing World, Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, available at: https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

[610] Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court, Privacy and Civil Liberties Board, available at: https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf

The use of data acquired by Bulk Communications Data for target development or to "understand relationships between suspects in a way that would not be possible using only targeted communications data powers" should be prohibited. Only specific queries, relating to an identifiable target, should be permitted.

There should be an examination regime for access to any Communications Data, regardless of where or how it was obtained. The lack of examination regime surrounding Bulk Communications Data Acquisition is a notable absence, and it is an important safeguard that exists in all the other bulk power regimes.

Bulk Personal Datasets

Almost nothing is known about Bulk Personal Datasets (BPDs), including what exactly they are, or how they are used. BPDs have been officially described as being comprised of *"data that contain personal information about a wide range of individuals, the majority of whom are unlikely to be of any intelligence interest."*[611] The little else that is known suggests the Committee should act with great caution, as Bulk Personal Datasets may end up being the most intrusive and least regulated power being proposed in this draft Bill.

I set out what is publicly known about BPDs in more detail at **Annex D**.

Occasionally, intelligence service staff point to the richness of data held, with consent, by technology and internet companies. Former Director of GCHQ Iain Lobban told the Telegraph "*Who has the info on you? It's the commercial companies, not us, who know everything.*[612]" With Bulk Personal Datasets, intelligence agencies are forcing numerous companies to hand over everything they know, in bulk, to allow the agencies to combining the knowledge of multiple commercial companies in a single place.

From there, these "*millions of records*" are "*linked together so that analysts can quickly find all the information linked to a selector (e.g. a telephone number or a ***) from one search query.*"[613]

No formal oversight, prior to that initiated by the Prime Minister this year, has taken place, despite the conduct clearly affecting the civil liberties of British citizens.

---

[611] Arrangements for the Obtaining and Disclosing of Bulk Personal Datasets, available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473782/Handling_arrangements_for_Bulk_Personal_Datasets.pdf

[612] Charles Moore, GCHQ: 'This is not Blitz Britain. We sure as hell can't lick terrorism on our own', *The Telegraph*, available at: http://www.telegraph.co.uk/news/uknews/defence/11154322/GCHQ-This-is-not-Blitz-Britain.-We-sure-as-hell-cant-lick-terrorism-on-our-own.html

[613] Privacy and Security: A modern and transparent legal framework, Intelligence and Security Committee.

Abuse has already taken place. With the ISC reporting each of the three Agencies "*had disciplined – or in some cases dismissed – staff for inappropriately accessing personal information held in these datasets in recent years.*"

Without understanding which Bulk Personal Datasets have been acquired already, and which may be acquired in future, the scope of this power cannot be properly assessed. It is likely that medical records, including those from the NHS, could be acquired, in bulk, under this power. Likewise, travel and border records and financial records, including those from credit reference agencies, could be acquired, if they haven't been already.

BPDs have not been subjected to a single formal review or report and as a result, the proposed legal framework pertaining to BPDs is the least rigorous of all the bulk powers.

Conclusion and recommendations

Due to the lack of information being provided to assess what would be a power which could be used to obtain any dataset, regardless of size, sensitivity, or scope, and a lack of an operational case, the use of Bulk Personal Datasets should be prohibited

Although I make the above recommendation in the strongest terms, if Bulk Personal Dataset powers are retained in the draft Bill, the following minimum safeguards must be introduced into the legislation:

Lists of the Bulk Personal Datasets that have already been acquired should, where possible, be published. Where national security concerns are raised, the Government should publish information on broad categories of BPDs, such as "financial" or "medical", and the quantity of BPDs as well as the number of individual records contained within them should be published.

Criminal offences should be enacted for misuse of Bulk Personal Datasets, in the same way that there are statutory offences for misuse of intercepted material and communications data.

Bribing staff inside companies/organisations, placing human intelligence assets inside companies/organisations or obtaining Bulk Personal Datasets by any other covert means should be prohibited. Only overt methods, by legal compulsion, should be considered.

The Committee may wish to consider recommending language be introduced in the legislation to ensure that certain Bulk Personal Datasets that should never be obtained. An initial list could include medical information in bulk from the NHS and other health providers.

Bulk Personal Dataset warrants must describe specific individual datasets. Provisions in warrantry as per s.152(6) to allow warrants to authorise the obtaining, retention and examination of "replacement datasets" that do not exist at the time of the issue of the warrant should be removed.

There should be an examination regime for access to any Communications Data, regardless of where or how it was obtained. The lack of examination regime surrounding Bulk Communications Data Acquisition is a notable absence, and it is an important safeguard that exists in all the other bulk power regimes.

Conclusion

The capabilities contained within this draft Bill are extraordinary. This is the first time that Parliament has ever been given the opportunity to debate the necessity of, or the operational case for, many of the most intrusive powers in this Bill. I hope this opportunity will be exploited to its fullest.

Only the restrictive word count and short submission timeframe prevented me from addressing other problematic areas of this draft Bill. My silence on them in this report should not be taken as a lack of concern. I trust others will have be able to address them in their submissions.

If there is any further information the Committee requires, I would be happy to assist however I can.

December 2015

Annex A - Bulk Interception

Operating primarily out of Bude in Cornwall, the GCHQ mass surveillance programme TEMPORA includes the first "full take" internet fibre-optic interception site anywhere in the world and purportedly provides the single "*biggest internet access*" enjoyed by any intelligence agency worldwide.[614] Indeed, the vast number of private communications being intercepted requires a special kind of processing known as "Massive Volume Reduction" to make sense of the collected private communications. In 2009, internal GCHQ documents stated "*this massive site uses over 1000 machines to process and make available to analysts more than 40 billion piece of content a day*."[615]

The volume of data collected is enormous and so most of the material cannot be reviewed by a person. At such a scale, it is impossible to immediately determine what will be of interest to GCHQ, nor is it possible to immediately filter out the private communications of perfectly innocent people who are not suspected of anything. Instead, GCHQ treats every piece of information intercepted as potentially suspicious, pieces it back together, and subjects it to intrusive processing, filtering, and analysis. GCHQ then mines the data for correlations and patterns, suspicious words or phrases, relationships or connections using powerful computers, building profiles on people automatically.

[614] "TEMPORA – The World's Largest XKEYSCORE", *Der Spiegel,* available at: http://www.spiegel.de/media/media-34090.pdf

[615] "TEMPORA – The World's Largest XKEYSCORE", *Der Spiegel,* available at: http://www.spiegel.de/media/media-34090.pdf

In this way, the private communications of everyone who is caught up in this net are the subject of experimentation in an attempt to determine how suspicious a certain person, about whom nothing previous was known, may or may not be. Emails between close friends, phone calls between family members, internet searches about medical conditions, and the browsing of news websites for political views will all be examined and graded.

One programme, KARMA POLICE, used the communications captured in bulk to provide the agency with "*a web browsing profile for every visible user on the Internet*."[616] The individuals whose communications were intercepted, and had profiles built about them, were not specifically named in or targeted by interception warrants; rather, the collection is constituted from "unselected" or "untargeted" material. This is not mere passive collection and storage of private communications, but an active attempt to build detailed profiles, akin to a physical dossier or file on everyone on the internet, based on individuals' web searches. As extraordinary as it sounds, nevertheless, this was the stated goal of the GCHQ programme.

Under another programme, OPTIC NERVE, GCHQ intercepted substantial quantities of sexually explicit communications from private video conversations.[617] In one six month period in 2008, GCHQ collected webcam imagery from more than 1.8 million Yahoo user accounts globally. Rather than collecting webcam videos in their entirety, the programme saved one image every five minutes to avoid overloading GCHQ's servers. GCHQ also reportedly applied facial recognition technology to the collected video chats.

From the webcam imagery harvested by this programme, documents reveal that between 3% and 11% contained "undesirable nudity". The large amount of private sexually explicit webcam imagery was noted by GCHQ, and an internal guide explained to intelligence analysts that *"there is no perfect ability to censor material which may be offensive. Users who may feel uncomfortable about such material are advised not to open them*." The programme began in 2008 and was still active in 2012.

Even when data does not immediately yield interesting or useful intelligence, agencies seek to store as much of it as possible, with the intention of returning to it and applying retrospective analyses at some point in the future when it might be newly interesting or useful. The objective is to strive to build an ever-larger haystack, in order to improve both the intelligence agencies' current and future capacity to find needles. This mind-set, coupled with dramatically decreasing costs of data storage and exponentially increasing volumes of communications, has created what GCHQ's close partner NSA calls "*the golden age of SIGINT*."[618]

---

[616] Ryan Gallagher, "PROFILED From Radio to Porn, British Spies Track Web Users' Online Identities", *The Intercept*, available at: https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities/

[617] Ackerman and Ball, "Optic Nerve- millions of Yahoo webcam images intercepted by GCHQ," The Guardian (27 February 2014).

[618] Risen and Poitras, "N.S.A. Report Outlined Goals for More Power", *The New York Times,* (22nd November 2013) available at: http://www.nytimes.com/interactive/2013/11/23/us/politics/23nsa-sigint-strategy-document.html

The underpinning architecture, TEMPORA, is designed to act as an "Internet Buffer" that "*slows down a large chunk of Internet data*."[619] The goal is to allow intelligence agencies "retrospective analysis" of any communication they wish to examine that flows through the internet past their sensors. By deploying a high speed filtering and exploitation system called "XKEYSCORE" the agency is able to ingest, search and analyse exceptionally large quantities of private communications. When access to the GCHQ programme was first provided to NSA, it was described as "World's Largest" which "contains more data than all other XKEYSCORE'S combined" [620] and "more than 10 times larger than the next biggest XKEYSCORE."[621]

The Guardian reported that TEMPORA potentially gives GCHQ access to 21 petabytes of data a day. A petabyte is approximately 1,000 terabytes (which is in turn 1000 gigabytes). To put this in perspective, this is the equivalent of sending all the information in all the books in the British Library 192 times every 24 hours. In a presentation to GCHQ analysts, it was put simply that *"[t]his is a massive amount of data!*"[622]

Although Britain has a long history of gaining access to communications via the interception of undersea cables, the volume of communications that is being intercepted and analysed under TEMPORA is orders of magnitude greater than GCHQ's previous capacity. Despite efforts to downplay the scale of access GCHQ enjoys, around 25% of the worlds internet traffic flows through the UK. [623]

In 2009, this internet traffic flowed through around 1600 bearers[624] contained within undersea fiber optic cables. Internal documents explain that "*although the total percentage processed may seem in the lower percentile range we [GCHQ] can actually survey the majority of the 1600 […] This allows us to select the most valuable to switch into our processing systems*."[625]

The constraints and limitations on processing more bearers are mostly technical in nature and due to resourcing and other budgetary constraints, rather than any legal limits or issues of principle. The plan in one set of GCHQs document suggests that by March 2011, the number processed into GCHQ systems would rise to 415; more than a quarter of all bearers transiting the UK.[626]

---

[619] "TEMPORA – The World's Largest XKEYSCORE", *Der Spiegel,* available at: http://www.spiegel.de/media/media-34090.pdf

[620] "TEMPORA – The World's Largest XKEYSCORE", *Der Spiegel,* available at: http://www.spiegel.de/media/media-34090.pdf

[621] "TEMPORA – The World's Largest XKEYSCORE", *Der Spiegel,* available at: http://www.spiegel.de/media/media-34090.pdf

[622] MacAskill, Borger, Hopkins, Davies and Ball, "GCHQ taps fibre-optic cables for secret access to world's communications" *The Guardian,* (21st June 2013) available at: http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

[623] "200G IRIS Access", *The Intercept*, available at: https://theintercept.com/document/2015/09/25/200g-iris-access

[624] "200G IRIS Access", *The Intercept*, available at: https://theintercept.com/document/2015/09/25/200g-iris-access

[625] "200G IRIS Access", *The Intercept*, available at: https://theintercept.com/document/2015/09/25/200g-iris-access

[626] "200G IRIS Access", *The Intercept*, available at: https://theintercept.com/document/2015/09/25/200g-iris-access

As of May 2012, there has been a 7000 per cent increase in information obtained from fibre optic undersea cables[627] with TEMPORA capabilities at multiple processing centres based within the UK and overseas.[628]

One report heard evidence on this more specifically. The RUSI panel "*were told that the technical work that goes in before the actual interception takes effect is very important, in terms of minimising intrusion and ensuring that large amounts of incidental material are not intercepted*."[629] Despite this, there is nothing in the draft Bill that sets out that policy, or places any constraints on practice.

Annex B - Bulk Equipment Interference

Intelligence agencies have developed hacking techniques they call "Computer Network Exploitation" (CNE) or "Active Signals Intelligence" (Active SIGINT), which, NSA documents explain, "*offers a more aggressive approach to SIGINT. We retrieve data through intervention in our targets' computers or network devices. Extract data from machine*."[630] With these capabilities to infect devices with intrusive malware,[631] GCHQ hopes to be able to "*exploit any phone, anywhere, any time*."[632] A GCHQ document explains: "*if it's on the phone, we can get it*."[633]

> Hacking a mobile phone gives governments (or others) total control of features like the camera, microphone and keyboard, which may be utilised, manipulated and turned against the user of the device. Internal GCHQ documents explain that the agency is interested in "[n]ot just collecting voice and SMS and geo-locating phone, but getting intelligence from all the extra functionality that iPhones and BlackBerrys offer."[634]
>
> A suite of tools – codenamed WARRIOR PRIDE – is used by GCHQ to achieve some of these goals. This framework includes a range of capabilities: using DREAMY SMURF, GCHQ are able to turn on a mobile phone that is apparently switched off; NOSEY SMURF allows the agency to activate the device's microphone; and TRACKER SMURF

---

[627] Borger, J. and Hopkins, N. (1 August 2013) Exclusive: NSA pays £100m in secret funding for GCHQ, *The Guardian* [Online]. Available from: http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden [Accessed 1 October 2015]

[628] GCHQ Wiki entry on TEMPORA, *Der Spiegel*, available at http://www.spiegel.de/media/media-34103.pdf

[629] A Democratic Licence to Operate, Report of the Independent Surveillance Review, *RUSI*, available at: https://rusi.org/sites/default/files/20150714_whr_2-15_a_democratic_licence_to_operate.pdf

[630] Intelligent Command and Control (15 March 2014) [Online]. Available from: https://www.eff.org/files/2014/04/09/20140315-intercept-turbine_intelligence_command_and_control.pdf [Accessed 1 October 2015]

[631] Malware is specialized software that allows whoever deploys it to take control of or extract information from a target device. This is usually accomplished by circumventing any security software or other protections present on the device.

[632] Borger, J. and Hopkins, N. (1 August 2013) Exclusive: NSA pays £100m in secret funding for GCHQ, *The Guardian* [Online]. Available from: http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden [Accessed 1 October 2015]

[633] Capability - iPhone (28 January 2014) [Online]. Available from: http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data#img-3 [Accessed 1 October 2015]

[634] Borger, J., Harding, L. and Hopkins, N. (2 August 2013) GCHQ: inside the top-secret world of Britain's biggest spy agency, *The Guardian* [Online]. Available from: http://www.theguardian.com/world/2013/aug/02/gchq-spy-agency-nsa-snowden [Accessed 28 September 2015]

allows the agency to activate the device's GPS location tracker.[635] To ensure that the presence of malware is not detected, PARANOID SMURF helps the malware to remain hidden on the device.[636]

GCHQ is able to record every keystroke pressed on a device using QWERTY, designed to collect and exfiltrate all keyboard keys pressed by the victim and record them for later inspection.[637] This enables the agency to see everything that the user has typed, including not just the contents of communications and documents, but also any text that was subsequently deleted, and any passwords that the user entered.

When CNE is targeted against networks, matters get more complex. In the words of an NSA analyst, "*there are a plethora of things you could do once you get CNE access to a router…suffice it to say, getting access to a router is very good for the actor, and very bad for the victim*."[638]

Far from being a capability of last resort for extreme circumstances, it appears this kind of large-scale attack against networks are being deployed regularly against both company and country communications networks. As one document explains "*Hacking routers has been good business for us and our 5-eyes [sic] partners for some time*."[639]

Telecommunications companies are often the targets of these attacks. Just within Germany, several communications have been compromised by GCHQ. Deutsche Telekom AG, which provides mobile phone, internet and landline service to 60 million people in Germany, was hacked by GCHQ.[640] Likewise, Netcologne, which operates a fiber-optic network and provides telephone and internet services to 400,000 customers, was targeted by GCHQ, as were German satellite operators Stellar, Cetel, and IABG.[641]

---

[635] Ball, J. (28 January 2014) Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data, *The Guardian* [Online]. Available from: http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data [Accessed 28 September 2015]

[636] Ball, J. (28 January 2014) Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data, *The Guardian* [Online]. Available from: http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data [Accessed 28 September 2015]

[637] Malware from the Five Eyes (27 January 2015) [Online]. Available from: http://www.spiegel.de/media/media-35668.pdf [Accessed 28 September 2015]

[638] Targeting System Administrator Accounts to Access Networks (20 March 2014) [Online]. Available from: https://www.eff.org/files/2014/04/09/20140320-intercept-targeting_system_administrator_accounts.pdf [Accessed 28 September 2015]

[639] Five Eyes Hacking Large Routers (12 March 2014) [Online]. Available from: https://www.eff.org/files/2014/04/09/20140312-intercept-five_eyes_hacking_large_routers.pdf [Accessed 28 September 2015]

[640] Grothoff, C. et al (14 September 2014) Map of the Stars: The NSA and GCHQ Campaign Against German Satellite Companies, *The Intercept* [Online]. Available from: https://firstlook.org/theintercept/2014/09/14/nsa-stellar/ [Accessed 1 October 2015]

[641] Grothoff, C. et al (14 September 2014) Map of the Stars: The NSA and GCHQ Campaign Against German Satellite Companies, *The Intercept* [Online]. Available from: https://firstlook.org/theintercept/2014/09/14/nsa-stellar/ [Accessed 1 October 2015]

These companies are not considered national security threats nor are they suspected as being involved in crime. Instead their networks are attacked and their employees targeted because they are seen as a means to an end.

Once on their networks, there are a range of activities that can be undertaken. Communications traffic can be redirected in bulk, as a 2008 warrant explains: *"[o]ur presence on routers likewise allows us to re-route selected traffic across international links towards passive collection systems*."[642]

Another reason why GCHQ attacks networks is to use the network as a launching pad for further attacks. GCHQ's deployment of CNE against Belgium's largest telecommunications provider, Belgacom, suggests the ultimate goal was to "*enable CNE access to BELGACOM Core GRX Routers from which we can undertake MiTM [man-in-the-middle] operations*[643] *against targets roaming using Smart Phones*."[644] In other words, GCHQ wanted to use Belgacom's network to launch further CNE operations against phones that used the network.[645]

In some circumstances, documents show intelligence agencies undertake what they call "*supply chain enabling, exploitation, or intervention operations*" including *"[h]ardware implant enabling exploitation or operations.*"[646] Interfering with the network hardware supply chain in this way allows intelligence agencies to place controlled backdoors in the "*internet backbone*"[647] and gain access to communications networks, providing potential access to a whole country's core communication infrastructure used by millions of people.[648]

GCHQ use a variety of methods to exploit hardware and software. Many of those methods rely on the use of a vulnerability – a pre-existing error, often called a "bug" or in hardware or software that allows it to be used in a manner that was not intended or anticipated. Zero day vulnerabilities get their name from the fact that, when identified, the computer user has had "zero days" to fix them before attackers can exploit the vulnerability. By purchasing zero days, and using them offensively as

---

642 GCHQ Application for Renewal of Warrant GPW/1160 (22 June 2015) [Online]. Available from: https://theintercept.com/document/2015/06/22/gchq-warrant-renewal/ [Accessed 1 October 2015]

643 A "man in the middle" attack deploys malware without the active participation of the target. The attack interrupts, or gets in the middle of, a request by the target device to access internet content. For instance, a target computer might be requesting to connect to a particular website. The agent will intercept that request, and respond to it, often by impersonating the website. In their response, the agent will send back malware instead of, or sometimes in addition to, the requested content.

644 Operation Socialist (24 October 2013) [Online]. Available from: https://www.eff.org/files/2013/11/15/20130920-spiegel-belgacom.pdf [Accessed 1 October 2015]

645 Gallagher, R. (13 December 2014) Operation Socialist: The Inside Story of How British Spies Hacked Belgium's Largest Telco, *The Intercept* [Online]. Available from: https://firstlook.org/theintercept/2014/12/13/belgacom-hack-gchq-inside-story/ [Accessed 1 October 2015]

646 Computer Network Exploitation Classification Guide / 2-59 [Online]. Available from: http://www.spiegel.de/media/media-35656.pdf [Accessed 2 October 2015]

647 Stealthy Techniques Can Crack Some of SIGINT's Hardest Targets (17 January 2015) [Online]. Available from: https://www.eff.org/files/2015/01/27/20150117-spiegel-supply-chain_interdiction_-_stealthy_techniques_can_crack_some_of_sigints_hardest_targets.pdf [Accessed 28 September 2015]

648 Stealthy Techniques Can Crack Some of SIGINT's Hardest Targets (17 January 2015) [Online]. Available from: https://www.eff.org/files/2015/01/27/20150117-spiegel-supply-chain_interdiction_-_stealthy_techniques_can_crack_some_of_sigints_hardest_targets.pdf [Accessed 28 September 2015]

part of attacks, GCHQ are preventing preventing potentially millions of individuals and companies from being protected.

In the normal course, when researchers and others discover vulnerabilities, they report the vulnerability to the company responsible for the security of the equipment affected. If GCHQ discover a vulnerability, however, they have an incentive not to reveal it in order to use it offensively as part of a CNE attack, or to stockpile it for future use. An NSA classification guide states that "technical details concerning specific software vulnerabilities, when not publicly known, and [that] are exploited for CNE activities" hold a minimum classification of TOP SECRET.[649]

Even at the law enforcement level, zero days are being used. Companies trying to sell malware to law enforcement bodies, including National Crime Agency, use zero days in their products[650]. Recently the FBI confirmed that malware they deploy also makes use of zero day vulnerabilities.[651]

This perverse situation has drawn criticism in the US, from the President's own Review Group on Intelligence and Communications Technologies. When considering the zero day problem, the Review Group recommended that *"[i]n almost all instances, for widely used code, it is in the national interest to eliminate software vulnerabilities rather than to use them for US intelligence collection. Eliminating the vulnerabilities — 'patching' them — strengthens the security of US Government, critical infrastructure, and other computer systems*."[652]

Unintended consequences of CNE

Unlike more traditional SIGINT collection techniques that acquire communications passively, the active intervention of CNE is fraught with difficulties.

Occasionally, unintended consequences occur when targeting large scale, core communications infrastructure with CNE. In 2012, it was reported that 92 per cent of the communications networks providing internet connectivity to Syria were suddenly knocked offline.[653] At the time, this disruption was widely assumed to have been caused by the Syrian government in order to destabilise opposition groups, and was criticised by world leaders.

According to Edward Snowden, however, the NSA, not the Syrian government, caused the disruption. The NSA had been attempting to use CNE to conduct surveillance on the Syrian network when something went wrong with the operation "*and the [targeted] router was bricked instead—rendered totally inoperable. […] The failure of this router caused Syria to suddenly lose all connection to the internet –*

[649] NSA Budget on Computer Network Operations - Code Word GENIE (17 January 2015) [Online]. Available from: https://www.eff.org/files/2015/02/03/20150117-spiegel-excerpt_from_the_secret_nsa_budget_on_computer_network_operations_-_code_word_genie.pdf [Accessed 1 October 2015]

[650] http://www.wired.com/2015/07/hacking-team-leak-shows-secretive-zero-day-exploit-sales-work/

[651] http://fortune.com/2015/12/09/fbi-zero-day/

[652] President's Review Group on Intelligence and Communications Technologies (12 December 2013) Liberty And Security in a Changing World [Online]. Available from: https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [Accessed 1 October 2015]

[653] Shachtman, N. (29 November 2012) Syria Has Just Been Taken Offline, *Wired* [Online]. Available from: http://www.wired.com/2012/11/syria-offline/ [Accessed 1 October 2015]

although the public didn't know that the US government was responsible."[654]

Other issues also occur, such as malware spreading beyond its intended target, as was the case when Iranian nuclear facilities were targeted by Stuxnet; other companies such as Chevron were caught up in the attack. The CIO of the Chevron put it plainly: "*We're finding it in our systems and so are other companies [. . .] [s]o now we have to deal with this*." [655]

It also appears to be hard to remove malware from computer systems once it has been deployed. One set of researchers who examined Five Eyes malware, found that despite the fact that a CNE attack occurred over 12 years ago, victim computers around the world were still infected with the malware, with dozens of them continuing to transmit information back from around the world.[656]

Scale of CNE deployments

CNE was once a rarely used capability, but this did not stay the case for long. In the United States, by 2003, the use of CNE had risen dramatically, and with a few hundred NSA staff conducting on average 20-25 CNE operations a day, rising again to 100 CNE operations a day by the end of 2005.[657]

Since then the Five Eyes have "aggressively scaled"[658] their hacking initiatives, in the past decade computerizing some processes previously handled by humans. One key system codenamed TURBINE now "*allow[s] the current implant network to scale to large size (millions of implants) by creating a system that does automated control implants by groups instead of individually*."

Another document confirms the scale of the ambition, stating TURBINE's goal is to "*increase the current capability to deploy and manage hundreds of Computer Network Exploitation (CNE) and Computer Network Attack (CNA) implants to potentially millions of implants*."[659] Developed as part of the Tailored Access Operations unit, the TURBINE system is described in leaked documents as an "*intelligent command and control capability*" that enables "*industrial-scale*

[654] Ackerman, S. (13 August 2014) Snowden: NSA accidentally caused Syria's internet blackout in 2012, *The Guardian* [Online]. Available from: http://www.theguardian.com/world/2014/aug/13/snowden-nsa-syria-internet-outage-civil-war [Accessed 1 October 2015]
[655] King, R. (9 November 2012) Virus Aimed at Iran Infected Chevron Network, *The Wall Street Journal*. Available from: http://www.wsj.com/articles/SB10001424127887324894104578107223667421796 [Accessed 1 October 2015]
[656] Goodin, D. (16 February 2015) How "omnipotent" hackers tied to NSA hid for 14 years—and were found at last, *Ars Technica* [Online]. Available from: http://arstechnica.com/security/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/ [Accessed 1 October 2015]
[657] Expansion of the Remote Operations Center (ROC) on Endpoint Operations (17 January 2015) [Online]. Available from: https://www.eff.org/files/2015/01/23/20150117-speigel-document_about_the_expansion_of_the_remote_operations_center_roc_on_endpoint_operations.pdf [Accessed 2 October 2015]
[658] Gallagher, R. and Greenwald, G. (12 March 2014) How The NSA Plans To Infect 'Millions' Of Computers, *The Intercept* [Online]. Available from: https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/ [Accessed 28 September 2015]
[659] Gallagher, R. and Greenwald, G. (12 March 2014) How The NSA Plans To Infect 'Millions' Of Computers, *The Intercept* [Online]. Available from: https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/ [Accessed 28 September 2015]

exploitation."[660]

It is unclear how many devices the Five Eyes have interfered with over the years. The Washington Post reported that the LinkedIn profile of one NSA staffer included the fact that the 14 personnel under his command had undertaken over 54,000 CNE operations.[661] I imagine the total number must be in the millions.

Equipment Interference and Bulk Equipment Interference will likely continue to be deployed in this way, and continue to scale, infecting computers and networks many of which are not an intelligence target themselves, are not a threat to national security, nor suspected of any criminal wrongdoing.

Despite the agencies' clear existing CNE capabilities, there is currently no clear statutory authority and Parliamentary consent for the them to undertake Computer Network Exploitation.

CNE code review

In Germany, the use of malware has been contested for many years. In 2008, the German constitutional court created a new computer basic right for "*fundamental right to ensure the confidentiality and integrity of information technology systems*" which imposed restrictions that that must be ensured both in by legal processes but also technically.

German authorities reassured concerned parties that malware would be "hand-crafted" for the specifics of each case and would meet strict levels of quality control, not least because of the active nature of computer network exploitation the risk for things to go wrong is high.

Despite these reassurance, security researchers who were able to obtain copies of the trojan used by Germany authorities found that the design and implementation of the trojan used "*lacked basic safety requirements*".[662] They concluded that "*the government malware can, unchecked by a judge, load extensions by remote control, to use the trojan for other functions, including but not limited to eavesdropping. This complete control over the infected PC – owing to the poor craftsmanship that went into this trojan – is open not just to the agency that put it there, but to everyone. It could even be used to upload falsified "evidence" against the PC's owner, or to delete files, which puts the whole rationale for this method of investigation into question. […] Not only can unauthorized third parties assume control of the infected system, but even attackers of mediocre skill level can connect to the authorities, claim to be a specific instance of the trojan, and upload fake data. It is even conceivable that the*

[660] Gallagher, R. and Greenwald, G. (12 March 2014) How The NSA Plans To Infect 'Millions' Of Computers, *The Intercept* [Online]. Available from: https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/ [Accessed 28 September 2015]

[661] Peterson, A. (29 August 2013) The NSA has its own team of elite hackers, *The Washington Post* [Online]. Available from: https://www.washingtonpost.com/news/the-switch/wp/2013/08/29/the-nsa-has-its-own-team-of-elite-hackers/ [Accessed 2 October 2015]

[662] https://netzpolitik.org/2013/leistungsbeschreibung-wie-das-bundeskriminalamt-versucht-die-quellen-tku-gesetzeskonform-zu-machen/

law enforcement agencies' IT infrastructure could be attacked through this channel."[663]

In response, a standardised terms of reference[664] was created to define technical specifications which had to be met by the trojans to be compliant with the constitutional and statutory requirements. This includes a source code audit and function test by an outside party. While criticised as not going far enough,[665] an independent review of malware used would be a welcome first step to protect against abuse.

Impairment of forensic evidence

With the deployment of CNE inside the United Kingdom by security agencies or law enforcement bodies, principles pertaining to the integrity of computer evidence fall into question. Any intrusion into a computer will necessarily result in a change to the contents of the device unless the most stringent precautions are taken. As a result, access to a computer or device via CNE prior to the seizure of a device, makes a mockery of the the precautions usually followed by law enforcement when copying hard drives such as the the use of write-protect devices. The risk, if there is an eventual criminal prosecution, is of potential defence accusations of evidence tampering. There is nothing in the proposed Bill, or public statements by the Home Office on this point, that reassures me that the use of CNE will not result in the automatic exclusion of material that otherwise would have been relied on in evidence.

Targeting innocents

The Draft Equipment Interference Code of Practice permits the targeting of "individuals who are not intelligence targets in their own right." This will allow GCHQ to undertake missions against those who are not a national security threat, not suspected of any crime, or any other wrongdoing. This is plainly inappropriate.

Annex C - Bulk Acquisition

The use of Bulk Communications Data Acquisition to collect domestic phone records in bulk and subject them to data mining has until recently been kept secret. Nick Clegg MP stated that even inside Government "only a tiny handful of senior cabinet ministers" knew.[666] The Home Secretary only avowed[667] to Parliament the fact that MI5 were relying on an obscure statutory provision contained within Telecommunications Act 1984 in November 2015. When announced, David Anderson QC told the BBC that the "*law was so broad and the information was so slight that nobody knew it was happening*". He added it was "*so vague that anything could be done under it*."[668]

[663] http://ccc.de/en/updates/2011/staatstrojaner

[664] https://fragdenstaat.de/files/foi/8095/leistungsbeschreibung-quellen-tku.pdf

[665] https://netzpolitik.org/2013/leistungsbeschreibung-wie-das-bundeskriminalamt-versucht-die-quellen-tku-gesetzeskonform-zu-machen/

[666] http://www.theguardian.com/world/2015/nov/05/nick-clegg-cabinet-mass-surveillance-british-spying

[667] Gordon Corera, "MI5 'secretly collected phone data' for decade," *BBC News*, available at: http://www.bbc.co.uk/news/uk-politics-34729139

[668] http://www.bbc.co.uk/news/uk-politics-34729139

Transparency and oversight

Attempts to subject the power to oversight have only just begun. The Interception of Communications Commissioner (IOCCO) was asked to oversee s.94 of the Telecommunications Act 1984 by the Prime Minister. IOCCO has not yet been able to report back on the use of the power. As its more recent report explains *"[t]he challenges stem from the fact that the directions are secret as allowed for by statute, can be given by any Secretary of State and do not automatically expire after a certain period. There does not appear to be a comprehensive central record of the directions that have been issued by the various Secretaries of State. My office is therefore not yet in a position to be able to say confidently that we have been notified of all directions*."[669]

It is not known what directions have been made under the provision. Telecommunications companies must retain telephone and internet metadata records, as required previously under the Data Retention Directive and now under the Data Retention and Investigatory Powers Act. The telephone metadata records include who called whom, location, and length of phone calls. Internet metadata records include billing records, and assigned IP addresses.

Statements by Nick Clegg MP suggest it was these records, among others, that may have been acquired in bulk. He stated "*previous government had granted MI5 direct access to records of millions of phone calls made in the UK*."[670] The lawfulness of the power is currently being considered by the Investigatory Powers Tribunal in a claim brought by Privacy International.[671]

Due to the extreme secrecy that surrounded the power, neither the Anderson, ISC, or RUSI report devoted more than a couple of paragraphs to the capability. As such no operational case has ever been made, no detailed independent review or assessment made of the effectiveness, or usefulness of the capability.

Comparison to Section 215 Patriot Act

Helpfully, a comparison to the likely use of Bulk Communications Data Acquisition can be drawn from the United States, where the equivalent authority has been the centre of prolonged public debate and scrutiny.

On June 5, 2013, The Guardian published an article based on documents provided by Edward Snowden, a contractor for the NSA, which revealed the fact that NSA was running a bulk domestic telephone records program to the public. It subsequently became apparent that the US Foreign Intelligence Services Court had, in secret, accepted the government's argument that the phrase "relevant" contained with s.215 of the USA PATRIOT Act could be reinterpreted to expand authority from compelling phone companies to hand over individual specific phone records, to hand over all phone records they held. Multiple orders were made to multiple phone companies which were renewed every 90 days.

It is thought that the scope of the s.215 USA PATRIOT Act program was narrower, and less intrusive than what could be possible under s.94 of the Telecommunications Act. This

[669] http://www.iocco-uk.info/docs/2015%20Half-yearly%20report%20(web%20version).pdf
[670] http://www.theguardian.com/world/2015/nov/05/nick-clegg-cabinet-mass-surveillance-british-spying
[671] https://privacyinternational.org/node/670

includes the fact that "cell site location information" was not provided by the phone companies, something that is possible under s.94 , and NSA policy was not to subject the material to data mining, something that the ISC has confirmed UK security and intelligence agencies undertake.

The US intelligence community put forward strong arguments for keeping the s.215 USA PATRIOT Act authority, despite public pressure. To bolster their position, they compiled a list of fifty-four counterterrorism events in which s.215 USA PATRIOT Act "contributed to a success story."

Two independent bodies undertook reviews relating to this powers, and to determine in part whether the case studies put forward were credible and accurate. They immediately determined that, in fact, only twelve of the fifty-four counterterrorism events cited had any relevance to s.215.

With access to classified material, the President's Review Group on Intelligence and Communications Technologies concluded that "*Our review suggests that the information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders*".[672]

The Privacy and Civil Liberties Oversight Board concluded in the same manner: "[…] *the Section 215 program has shown minimal value in safeguarding the nation from terrorism. Based on the information provided to the Board, including classified briefings and documentation, we have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist polite or the disruption of an attack."*[673]

Subsequently, the US Court of Appeals for the Second Circuit considered the statutory and constitutional validity of the section 215 programme in the case of *ACLU v Clapper,*[674] and concluded that the 215 collection programme was not authorised by statute, and could not be unless "preceded by substantial debate, and expressed in unmistakeable language".[675]

In June 2015, the US Senate passed USA FREEDOM Act,[676] which ended the collection of bulk domestic phone records (with a 180-day grace period granted for compliance). Just a few weeks ago, the programme was confirmed to have ended[677] with the Office of the Director of National Intelligence stating "beginning Sunday,

[672] https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf
[673] https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf
[674] Decision of 7 May 2015.
[675] At p. 74.
[676] http://www.theguardian.com/us-news/2015/jun/02/congress-surveillance-reform-edward-snowden
[677] http://motherboard.vice.com/read/the-nsas-controversial-phone-surveillance-program-ends-on-saturday

November 29, the government is prohibited from collecting telephone metadata records in bulk under Section 215, including of both U.S. and non-U.S. persons."[678]

Given the conclusion of two independent reports, who had access to classified material, into the usefulness of a directly similar power found them ineffective and disproportionate, the presumption must be that Bulk Communications Data Acquisition is equally inadequate.

Annex D - Bulk Personal Datasets

Almost nothing is known about Bulk Personal Datasets; what they are, or how they are used. They have been officially described as holding "data that contain personal information about a wide range of individuals, the majority of whom are unlikely to be of any intelligence interest."[679] The little else that is known suggests the committee should act with great caution, as Bulk Personal Datasets may end up being the most intrusive and least regulated power being proposed in this draft Bill.

One reason that such poor regulation is being proposed in relation to them, is because historically, the regulation and scrutiny BPDs have been subjected to has been essentially non-existent. It was not until the March 2015 publication of the Intelligence and Security Committee's report[680] earlier this year that any reference to Bulk Personal Datasets was made. In that report the ISC expressed his criticism in the highest terms

On the same day as the ISC Report was published, the Prime Minister signed the Intelligence Services Commissioner (Additional Review Functions) (Bulk Personal Datasets) Direction 2015. The Direction places the review of Bulk Personal Datasets by the Intelligence Services Commissioner onto a statutory basis. This was the first time they were to be formally reviewed.

What is known

The ISC gave the following explanation of Bulk Personal Datasets:

> Bulk Personal Datasets are "*large databases containing personal information about a wide range of people*" (p. 55).
>
> Bulk Personal Datasets are used to identify subjects of interest, establish links between individuals and groups and improve understanding of a target's behaviour and connections, and to verify information obtained from other sources (p. 55).

---

[678] http://icontherecord.tumblr.com/post/134069716908/odni-announces-transition-to-new-telephone

[679] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473782/Handling_arrangements_for_Bulk_Personal_Datasets.pdf

[680] Privacy and Security: A modern and transparent legal framework, Intelligence and Security Committee, available at: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.pdf?attachauth=ANoY7cogxIxISwTX3oFpCeqtndWLjWhuweNYm55N-BdQGPFGP8QonY-wMwG4JlARy9DJ5dis55bZa8fdgID6fAO9EqYfeOWoMtTo0ZxG_wj8nELbqgDhIk3xaUwisDR0AYy227va0w5T2kTqQ8zGvyKftiwF0aZUla8h9o3iGMI6g3jrfjcAwgrLqgYS2FkNWMz-po3T0I6EKVSAGw_9N-7eIQyHkd2_pYw95rwRLfbnSa12Z-2E_DDrzOR1QH-RfR9ZlXt91q2T&attredirects=0

The collection and search of Bulk Personal Datasets "*may be highly intrusive and impacts upon large numbers of people*" (p. 59Y).

Bulk Personal Datasets vary in size "*from hundreds to millions of records*" and may be "*linked together so that analysts can quickly find all the information linked to a selector (e.g. a telephone number or a ***) from one search query*" (§156).

Bulk Personal Datasets affect British citizens ("*may include significant quantities of information about British citizens*" and "*none of the Agencies was able to provide statistics about the volume of personal information about British citizens that was included in these datasets*") (§158 and fn 142).

Abuse

Abuse has already taken place. With the ISC reporting each of the three Agencies "*had disciplined – or in some cases dismissed – staff for inappropriately accessing personal information held in these datasets in recent years.*" While attempts to place this power now in statute, it is difficult to see how this new legal framework will reduce the likelihood of future abuse.

Intelligence sharing

Existing practice is that entire Bulk Personal Datasets, including those relating to British citizens may be shared with foreign intelligence agencies. When shared, not even minimal safeguards apply. As the ISC explains "… *while these controls apply within the Agencies, they do not apply to overseas partners with whom the Agencies may share the datasets.*" There doesn't appear to be any new safeguards in the bill to remedy this. Given the relationship our intelligence agencies enjoy within the Five Eyes, it is assumed a number of Bulk Personal Datasets will have been shared with the alliance by default.

It is possible that a very large number of Bulk Personal Datasets have already been acquired by the security and intelligence agencies. The newly published Arrangements for the Obtaining and Disclosing of Bulk Personal Datasets[681] provide no specific numbers, but leave the impression that acquisition and the loading of datasets into analytical systems may be being done at the level of individual intelligence officers.

Lack of information

I note Committee members[682] have sought to find out which Bulk Personal Datasets have been acquired already, and which may be acquired in future. Privacy International[683] in their legal challenge in the Investigatory Powers Tribunal have

681 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473782/Handling_arrangements_for_Bulk_Personal_Datasets.pdf

682 https://twitter.com/LordStras/status/673435549194166272

683 https://privacyinternational.org/sites/default/files/Bulk%20Personal%20Datasets%20Grounds%20FINAL_0.pdf

speculated what such Bulk Personal Datasets could contain. Just three examples are excerpted below:

> **Medical records**
> Databases such as those held by the NHSBSA Prescription Pricing Division hold all prescriptions written in England in the last five years. The NHS Personal Demographics Service, the national electronic database of NHS patients, could be acquired. The British Pregnancy Advisory Service, which is Britain's largest single abortion provider, holds hundreds of thousands of records for the 65,000 women they help each year. Private health records from BUPA, or Nuffield Health are growing in size.
>
> **Travel records**
> Many databases contain detailed personal travel records. Oyster card transactions provide a detailed map of movements throughout London and similar metrocard databases could be obtained for other cities. Centralised hotel reservation services, flight booking services, as well as car rental databases from companies like Sixt, Europcar, or Enterprise, all contain personal information on a large number of people that may be of interest to intelligence agencies.
>
> **Financial records and credit reference agencies**
> Credit reference agencies in the UK such as Experian, Equifax or Callcredit hold personal details of millions of people. These databases contain information such as loan borrowing and repayments, water and energy bills, payday loans, court records and fraud allegations. Some even include the angle of your garden, whether you have a burglar alarm fitted, the make and mileage of your car, how much you spend on wine, sports and vitamins, if you gamble, where you go on holiday and what you read.

In the new framework there is little on how the Bulk Personal Datasets would be compelled. Notably, the ISC report mentions covert action could used to acquire Bulk Personal Datasets[684]. At it's simplest, covert collection could take the form of the physical stealing of the data from a company. With the establishment of internal GCHQ HUMINT (human intelligence) Operations Team[685] whose who are tasked with "identifying, recruiting and running covert agents ," these traditional spying techniques are likely not to be ignored. Another common tactic used is bribery, with recent news showing the Drugs Enforcement Agency paid employees of foreign telecommunications firms for copies of similar databases. [686]

Occasionally, intelligence service staff point to the richness of data held, with consent, by technology companies. Former Director of GCHQ Iain Lobban told the Telegraph "*Who has the info on you? It's the commercial companies, not us, who know everything.*[687]" With Bulk Personal Datasets, intelligence agencies are able to

[684] ISC report, page 56
[685] http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security
[686] http://www.usatoday.com/story/news/2015/04/07/dea-bulk-telephone-surveillance-operation/70808616/
[687]

exploit that, combining the knowledge of multiple commercial companies into a single place.

Due to historic secrecy around the capability, the operational case for why Bulk Personal Datasets are necessary has never been made. They have not been subjected to a single formal review or report and as a result, the proposed legal framework is the least rigorous of all the bulk powers.

21 December 2015

http://www.telegraph.co.uk/news/uknews/defence/11154322/GCHQ-This-is-not-Blitz-Britain.-We-sure-as-hell-cant-lick-terrorism-on-our-own.html

Mr Gareth Kitchen—written evidence (IPB0059)

Executive Summary

- My concern is that the demands of the Draft Investigatory Powers Bill contravene EU Treaty obligations which the UK has a duty to enforce.
- I believe the concept of 'communication and traffic data' as defined in current Home Office guidance[688] and the Draft Bill does not accurately describe how the Internet functions and more importantly this guidance is out of step with definitions in the overarching EU directive[689].
- By following this guidance, industry unwittingly perpetuates the practice of casual interception and inspection of private communications and storage thereof, which contravenes both RIPA[690] and the EU directive.
- RIPA, by preventing both the prosecution and the defence from questioning the provenance of this intercepted evidence, fails to offer adequate safeguards, again contrary to EU directives.
- By extension, the proposal, in the draft bill, for bulk data retention is neither proportionate, time limited or with adequate safeguard also contrary to EU directives.

Personal Background

I have 30 years experience in the IT industry. I was the national support co-ordinator for a computer chain and a freelance IT consultant. For the last 15 years I have managed a small e-commerce business based in the Cotswolds. This business uses various servers and routing equipment, which I manage. Our business was the winner of the 2005 ecommerce awards, sponsored by the Department of Trade and Industry and BT.

Background

- There is widespread public disquiet about governmental overreach in terms of surveillance of citizens of both the UK and USA.
- The UK Government has responded by publishing the Draft Investigatory Powers Bill which claims to protect both privacy and security by improving transparency.
- The UK Government claims that the bill, building on RIPA (Regulation of Investigatory Powers Act 2000) only proposes to enhance powers in one area – that of communications data retention.
- It is proposed that information about internet services to which devices are connected (e.g. website, e-mail server or instant messaging application) will be stored by the communication service provider (CSP).
- As this data would be considered 'communication data' it may then be acquired from CSPs by law enforcement under RIPA.

[688] Home Office: Acquisition and Disclosure of Communications Data Code of Practice
[689] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0058
[690] http://www.legislation.gov.uk/ukpga/2000/23/contents

Introduction

6. I am submitting this evidence to the committee to provide insight into the way that devices connected to the Internet communicate.
7. I am concerned that Home Office guidance has stretched the accepted definition of Traffic Data in overarching EU Treaty to the point that the Draft Investigatory Powers Bill may compel UK Communication Service Providers (CSPs) to flout overarching EU Treaty obligations - obligations that the UK Government is entrusted to enforce.
8. I have carried out much research and sought advice from people in industry to support this evidence. I believe it all to be true and have provided links to the reference material I have drawn on.

EU Directive on Privacy and Electronic Communications

9. This directive requires UK Government to ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data without the consent of the users concerned691. There is, however, provision692 for the UK to restrict this requirement for a *limited time* in the interests of national security, defence, public security etc.
10. The directive still permits the UK Government to carry out lawful interception of electronic communications, but such measures must be appropriate and strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards.

EU Directive on Data Protection

11. To process or store personal data, this directive693 specifies that user consent must be 'freely given specific and informed'.

RIPA

1. RIPA, in its attempt to embrace the new digital modes of communication, defines various conceptual parts of a communication. The definitions, originally from the 2000 Act, have been enhanced694 in the draft bill, namely:-
   A. Traffic Data This is data that is or has been comprised in or attached to a communication for the purpose of its transmission. The Home Office guidance takes this a step further to suggest that 'traffic data' may identify a server or domain name but not a web page. This is a critical point.
   B. Communications Data The preface of the Draft Investigatory Powers Bill builds on the definition of Traffic Data to say that "Communications data is information about communications: the 'who', 'where', 'when', 'how' and 'with whom' of a communication but not what was written or said.". Indeed there has been much debate on the inclusion of the American term 'metadata' within the term 'Communications Data'. Recent government material695 shows that the term 'Communications Data Plus' has been

691 Article 5(1) of Directive 2002/58/EC
692 Article 15(1)
693 Article 2(h) of Directive 95/46/EC

694 Section 193
695 Intelligence and Security Committee of Parliament Privacy and Security: A modern and transparent legal framework

discussed, this concept would further extend the scope of what could be examined without actually disclosing the 'content' of the communication, encompassing details of web domains visited or the locational tracking information.

C. Internet Connect Record The same draft bill describes an Internet Connect Record as communication data stored to show the internet services a specific device has connected to, such as a website or instant messaging application. The suggestion is that the CSP's would be compelled to store this information. Clearly, this is very personal data.

Why define the data in this way?

1. Reading RIPA it becomes clear that the reason for this differentiation between different types of data, that form the communication, is so that access to the communication data can be sought by not only by law enforcement but other governmental organisations too.
2. It is proposed that communication data can be sought by a lowest tier of local Government with little oversight, whereas an actual Intercept warrant, to examine the content of the communication, would require a much higher level of authorisation.
3. For whatever reason, it is clear that the concept of communications data has been expanded in the Draft bill. Maybe legislators have become emboldened to do this as there have been no legal challenges to these concepts since RIPA was passed into UK law.
4. Curiously, the overarching EU Directive on privacy and electronic communications696 makes little distinction between types of data within a communication except for traffic data: "Traffic data may include any translation of this information by the network over which the communication is transmitted for the purpose of carrying out the transmission". Reassuringly, the Directive prohibits the listening, tapping, storage or other kinds of interception or surveillance of communications without the consent of the users concerned.

Shroud in secrecy

1. Legal opinion informs us that RIPA strives to prohibit the use of the fruits of intercept communications as evidence before courts. It does this by preventing both the prosecution and the defence from questioning the provenance of intercepted evidence.
2. The goal of RIPA is to 'shroud in secrecy many of the workings of the process of investigation'697.
3. As well as shrouding the workings of the investigation process RIPA therefore also prevents any definition of communications data or traffic data from being tested in a UK Court and gagging clauses within RIPA also prevent CSPs from making legal challenges.

Deep Packet Inspection

1. CSP's are always looking for value added services to offer their users. They may charge for these services or offer them freely in order to retain customers. A service filtering of web traffic for offensive material in order to protect children, for example.

---

696 http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0058

697 P Mirfield, 'Regulation of Investigatory Powers Act 2000: Part 2: Evidential Aspects' (2001) Criminal Law Review 91.

2. These services can only work at a CSP by using equipment that performs Deep Packet Inspection. Whereby, all traffic is intercepted and passed through a device and the communications are inspected and some decision is made based on the client and destination addresses. In the case of a service to protect children, the equipment may block access to a web site.
3. Without the 'freely given specific and informed' consent of the user any such service would be unlawful under RIPA Section 1 legislation and contrary to the obligations in the overarching EU Directive.

The Phorm Scandal[698]

1. In 2008 the Phorm scandal hit the headlines. Based on Deep Packet Inspection technology, the principle of what Phorm aimed to do was simple: it would intercept all of the web pages BT, TalkTalk and Virgin Media customers visited and scan them all of them for keywords in order to display targeted advertising on the client computer.
2. The European Commission was concerned Phorm was breaching EU privacy directives and called on the UK Government to take action to protect privacy. After unsatisfactory responses the EU eventually opened an infringement proceeding[699] against the United Kingdom.
3. Information Commissioner's Office (ICO) eventually ruled that Phorm's service must operate on an 'opt in' basis and the EU eventually dropped the infringement case in 2012.
4. The CPS was asked to investigate if there was sufficient evidence to prosecute under section 1 of the Regulation of Investigatory Powers Act (RIPA) 2000. But the CPS decided not to prosecute[700]. Curiously, one of the reasons cited was that The Home Office provided informal advice that stated that Phorm was unlikely to be contrary to section 1 of RIPA.
5. The actual informal advice which has been widely reported said "My personal view accords with yours, that even if it is 'interception', which I am doubtful of, it is lawfully authorised under section 3 by virtue of the user's consent obtained in signing up to the CSP's terms and conditions.
6. A cursory look at the current terms and conditions of some of the larger CSPs reveals the following broad statements about the service they offer:-
    a. VODAFONE: "We cannot guarantee the Service against unauthorised interruption or interception by third parties or that Services shall be error free and/or uninterrupted. You agree that your use of the Service is at your sole risk. The Company make no warranty that the Service will meet your requirements."
    b. TALK-TALK:"We try to keep your data and communications secure; however, for reasons beyond our control, these may be unlawfully intercepted. If they are, we'll investigate and advise on next steps."
7. These terms neatly comply with the overarching EU Directives and they do not, by default, opt-in their customers to any schemes or services.

[698] https://en.wikipedia.org/wiki/Phorm
[699] http://europa.eu/rapid/press-release_IP-10-1215_en.htm?locale=en
[700] http://blog.cps.gov.uk/2011/04/no-prosecution-of-bt-and-phorm-for-alleged-interception-of-browsing-data.html

8. So, the clear lesson learnt from the Phorm scandal was that services that process or store personal data must have user consent which must be '*freely given, specific and informed*'.

Evidence given to Parliament

1. During the Science and Technology Committee Meeting, 10th November 2015, the expert witnesses in the second panel demonstrated an impressive grasp of the concepts of the ethics of interception.
2. However, there was disagreement, over the Calendar example midway through the second session, by the experts. The disagreement centered on which part of the URL (web address) pointing to a calendar appointment was communication data and therefore valid to store and which was content and therefore invalid to store. Note the assumption that it is OK to store some of the communication!
3. I believe that their evidence is biased, as it relied on the concept of communication and traffic data as described in current Home Office guidance. I believe that the Home guidance definition of 'communication data' is inaccurate and out of step with definitions in the overarching EU treaty.
4. One could actually go so far to say that the term 'communication data' no longer carries any meaning with digital communications as there is no business justification for CSPs to create or store it. This seems to have been confirmed by industry evidence. This also explains why 'communication data' is not specifically mentioned in the overarching EU Treaty.
5. So, much of the discussion in all these consultations has centered about what is communication data and what is content. Again, industry consensus seems to be that there is little differentiation.
6. It has also become clear that the CSPs would have to upgrade their networks to enable them to capture communications data utilising Deep Packet Inspection technologies to fulfil the requirements of creating and storing these Internet Connection Records.
7. This is a fundamental point and raises a red flag for me! These Internet connection records can only be 'manufactured' at the CSP as a by-product of interception using deep packet inspection technologies. This, as per the Phorm Scandal, is simply not permitted under the EU Directive as the UK Government has to ensure the confidentiality of communications.
8. To further illustrate this, you can look at the e-mail and web-page examples given in Appendix 2&3. It is critically important to note the establishment of the reliable connection between the client and server, using TCP. This depth is often glossed over as being too technical for general discussion but it is fundamental to the operation of the network.

So what is content?

1. Armed with the information provided by the e-mail and web page examples in the appendix and the wording of the overarching EU directive it becomes a simple matter to identify traffic data in the communication.

2. The traffic data is merely the TCP connection data. Each client computer maintains a record of TCP connections, as does its local broadband router, as does

the e-mail or web server at the remote end. On a Windows machine you can use the command:-

netstat -p tcp

3. This command lists all the client computer's TCP connections along with the remote addresses and a hint about the type of service being used.

4. And this is the crux of the 'communication data'/content debate. Each device that participates in the communication needs a minimal amount of information to establish and maintain a reliable connection between both endpoints. This is the 'traffic data'. All other data that flows over the connection once it is established, whether encrypted or not, is 'content'.

5. So a log of TCP sessions (extracted close to the client router) could comprise :-

Date, Time, Source IP, Destination IP, Port
12-12-2015, 10:42:52, 198.81.25.26, 198.81.25.200, 25
12-12-2015, 10:42:52, 198.81.25.26, 183.81.25.321, 80
12-12-2015, 10:42:52, 198.81.25.26, 98.181.215.220, 80
12-12-2015, 10:42:53, 198.81.25.26, 8.1.2.222, 80
12-12-2015, 10:42:54, 198.81.25.26, 183.81.25.321, 80
12-12-2015, 10:42:55, 198.81.25.26, 98.181.215.220, 80
12-12-2015, 10:42:56, 198.81.25.26, 8.1.2.222, 443
12-12-2015, 10:53:53, 198.81.25.26, 8.1.2.222, 443
12-12-2015, 10:56:54, 198.81.25.26, 183.81.25.321, 443
12-12-2015, 10:57:55, 198.81.25.26, 98.181.215.220, 80
12-12-2015, 10:59:56, 198.81.25.26, 8.1.2.222, 443

6. This information would give the RIPA investigator the date-time and IP addresses and an indication about what type of communication was being made. I think it's a fair bet that pretty much any CSP could log this data, today, at their customer facing equipment.

7. Also, this log bears a striking similarity to an itemised telephone bill, which I find reassuring. No assumptions are made by the CSP as the data is raw, unprocessed and therefore true, unlike the envisaged CSP manufactured Internet Connect Records which would use third party lookup data etc. which may well introduce inaccuracies, assumptions and error.

8. Together, with a warrant, demands for this information by investigators would also appear proportionate.

Appendix 1
Timeline – Internet Evolution
I would like to lay out a number of points, that go back over my time in the industry and what I consider to be key points in the timeline:-

1. It is well established that with a warrant, post and telephone can be intercepted by law enforcement.
2. Law enforcement often request a log of phone call records from a CSP. This is data the company uses to calculate customer billing. Often described in TV drama.
3. The appropriate authorities can intercept any communication external to the UK, these powers are broad, intrusive and sweeping.
4. BT upgraded their analogue exchanges to digital with System X throughout the 1980's
5. HTTP 1.0 was defined in RFC 1945, May 1996. The World Wide Web was born.
6. During the early 1990's the use of SMTP and POP e-mail took off in the business environment. The e-mail servers were normally located within the business or at the CSP.
7. British Telecom upgraded their last electronic analogue exchanges to digital in 1998.
8. Hotmail acquired by Microsoft in 1998 with servers based in the USA.
9. Most internet traffic in those days was in the clear (plain text) so that if you put a packet sniffer on the network anyone could easily see any content in transit.
10. SSL the famous little padlock was released to the world in the late 90's as a means of providing secure data transmission between client and server computer thus facilitating the boom in e-commerce.
11. Carnivore, a CNE device installed at a CSP that could "sniff" traffic on a LAN segment looking for email messages in transit.
12. RIPA was passed into law in 2000 to ensure that the relevant investigatory powers are used in accordance with human rights.
13. Explosion of web sites and services most in the clear apart from e-commerce and banking.
14. Google launches Gmail in 2004.
15. 2008 the Phorm Scandal. A targeted advertising system introduced by BT, Talk Talk and others. The system intercepted the content of all of the web pages their customers visited and adverts were adjusted accordingly.
16. Google introduce SSL for Gmail.
17. 2009 The ICO confirm that any scheme such as Phorm must be 'opt-in' to comply with EU Law.
18. Microsoft introduces SSL for Hotmail in 2010.
19. RIPA guidance tightened to close loopholes around interception by private companies in 2011 in light of the Phorm scandal.
20. 2013 Edward Snowden revealed numerous global surveillance programs, many run by the NSA and Five Eyes with the cooperation of telecommunication companies and European governments.

Appendix 2
e-mail example
As the user clicks the send button on the client computer it would be helpful to recap how typical a typical e-mail is sent:-

First a small communication is sent to the DNS Server using a very simple protocol where there is no expectation that it will be received by the DNS Server. The client will only wait a short time for a response before trying a different server.

{Client sends a query to its DNS Server for the mail-server address}
C: 198.81.25.1,198.81.25.200,example.com,mx

This query meets the definition of a communication in the overarching EU Directive. As it is information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service.

{DNS Server sends a response back}
S: 198.81.25.200,198.81.25.26,mx

The client computer now knows the IP address of the mail server. Rather than blindly sending the contents of the e-mail as in the above example. The client has to establish and acknowledge a reliable connection on the servers port 25 (a well know port for sending mail).

So the client uses a more robust protocol called TCP to initiate a connection with the mail server. This process involves a well documented 3-way handshake[701] between the computers.

{Client initiates a TCP connection to 198.81.25.26 on port 25}

It may well be the case that this e-mail server supports Transport Layer Security. So, during the connection process this will be noted and keys exchanged to ensure that communication over the connection will be encrypted.

This is part of the communication that meets the definition of traffic data in the EU directive as it is data processed for the purpose of the conveyance of a communication on an electronic communications network.

Once the connection is established and acknowledged communication occurs over the connection as per the following example.

S: 220 smtp.example.com ESMTP Postfix
C: HELO relay.example.org
S: 250 Hello relay.example.org, I am glad to meet you
C: MAIL FROM:<bob@example.org>
S: 250 Ok

[701] https://support.microsoft.com/en-us/kb/172983

C: RCPT TO:<alice@example.com>
S: 250 Ok
C: RCPT TO:<theboss@example.com>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: From: "Bob Example" <bob@example.org>
C: To: "Alice Example" <alice@example.com>
C: Cc: theboss@example.com
C: Date: 6 Dec 2015 12:18:09 +0000
C: Subject: Test message
C:
C: Hello Alice.
C: This is a test message with 5 header fields and 4 lines in the message body.
C: Your friend,
C: Bob
C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye

{Server closes the TCP connection}

At this point the Mail Server adds a brief record of the conversation to the start of the e-mail (known as a header for human diagnostic purposes) and adds the message to its queue of work. This work would involve finding an appropriate Mail Server at example.org to take delivery of the message. Then a similar 'plain text' conversation would happen with that server, which would either take responsibility for delivering the message to alice and theboss or reject it.

Note that SMTP conveniently has a 'MAIL FROM', 'RCPT TO' in the header information, so if this information was logged by the CSP at their mail-server for their own business purposes, which in turn could be obtained under RIPA.

And so the industry assumes that any information after DATA is 'content' and information flowing before is the 'communication data'.

Whilst it may be possible to intercept and view this communication en-route to the mail-server it would be unlawful under RIPA and contrary to the EU Directive.

Appendix 3
web page example

{Client sends a query to its DNS Server for the web server address}
C: 198.81.25.1,198.81.25.200,examplesite.biz,a

This communication is sent to the DNS Server in the same way as the e-mail example.

{DNS Server sends a response back}
S: 198.81.25.200,68.81.95.2,a

The client computer now knows the IP address of the web server. However, rather than blindly requesting the contents of the web site, as with a DNS request, the client has to establish and acknowledge a reliable connection on port 80 (a well known port for web). As per the e-mail example a TCP connection is made with the web server.

{Client initiates a TCP connection to 68.81.95.2 on port 80}

It may well be the case that this web server uses https. During the connection process this will be noted and keys exchanged to ensure that communication over the connection will be encrypted.

Again, this part of the communication meets the definition of traffic data.

Once the connection is established and acknowledged communication occurs over the connection as per the following example.

C: GET /pages/policies/privacy.asp HTTP/1.1
C: host: www.examplesite.biz
C: <line feed>
S: HTTP/1.1 200 OK
S: Date: Mon, 18 Apr 2015 16:38:00 GMT
S: Server: IIS7 (Microsoft)
S: Last-Modified: Thu, 01 Jul 2015 01:16:05 GMT
S: Accept-Ranges: bytes
S: Content-Length: 6188
S: Connection: close
S: Content-Type: text/html
S:
S: <html>
S: <head>
S: <title>...
S: ...lots of HTML code here about site privacy...
S:
S: </body></html>

{Server closes the TCP connection}

It is interesting to note that there may be many unencrypted web sites sharing the IP address given to the client by the DNS server. So, the actual website address is again sent as part of the communication to the remote web server.

It must also be noted that as the client constructs the page on the client computer dozens of these 'pages' may be displayed as 'frames' within the overall page. Each 'frame' is treated in the same way as the main page where a DNS request is made and a TCP connection established then communication occurs and the results displayed.

20 December 2015

Martin Kleppmann—written evidence (IPB0054)

The rationale behind the proposed bill is presented as a choice between privacy and safety. Advocates of the bill argue that as a society, we must give up certain aspects of our privacy in order to ensure the safety of citizens. **This argument is false: the proposed bill would in fact harm the safety of citizens, not protect it.** It does not strengthen security at the cost of privacy: it is **harmful to both security and privacy**. It is a dangerous piece of legislation that must be entirely rethought.

In this document I will argue that the powers conveyed to the intelligence and law enforcement services in the proposed bill are not proportionate, not necessary, and in fact actively harmful to the interests of UK national security, UK businesses, and the safety of law-abiding citizens. The negative side effects of the bill far outweigh its benefits.

I am a researcher in the field of databases and information security, and an entrepreneur who has founded and sold two Internet businesses. This makes me intimately familiar with the technology issues related to this domain.

My greatest concern about the draft bill is with regard to the provisions for equipment interference (both targeted and bulk), and the provisions for interception of communication. In particular, service providers and manufacturers of equipment can be compelled to assist with the removal of electronic protection (see in particular sections 31, 101, 116, 145 and 189).

There is widespread uncertainty among software developers as to what technical measures precisely would be required in order to "assist" with the removal of protection, and whether certain technical measures such as end-to-end encryption would be considered a violation of this law. Neither the bill, nor the guidance notes, nor the statements from the government give sufficient technical detail. The evidence given by various researchers and software developers to the House of Commons Science and Technology Committee documents these concerns in detail.

Increasingly many software and communications products today are designed in such a way that the communication service provider cannot read the content of the communication. This is considered good security practice, because it protects against many security problems such as accidental exposure of data due to software bugs, leaks by malicious insiders, and attacks from hackers anywhere in the world. The inability to read the content of the communication is enforced through encryption (i.e. through mathematics, rather than mere policy, since policy is fallible but mathematics less so).

Conversely, if communication providers are required to assist with decrypting encrypted communications, that appears to imply that service providers must use protocols that can be decrypted in response to a warrant — that is, they cannot use encryption technologies in which the service provider is unable to assist with retrieving the content of the communication, because the mathematics makes it impossible.

Section 31 states that communication providers need only take "reasonably practicable" steps. Is it reasonable to require an operator to take a step that is mathematically

impossible? Probably not. However, 31(6) states that a step is reasonable by definition if it had been possible, had the operator complied with an order under section 189. Thus, an operator may be compelled under section 189 to make their software deliberately insecure, and then it would be reasonable to obtain the content of communication under the provisions of section 31. Moreover, software developers might choose to deliberately avoid security technologies pre-emptively, for fear that they might be subject to an order under section 189 in future, and the security technologies would make them unable to comply.

We can conclude that under the Investigatory Powers Bill, software developers would end up deliberately making their systems less secure than they could be, in order to be able to comply with the bill's provisions for "maintenance of technical capability". However, **deliberately weakening the security of computer systems would be a terrible mistake**.[702]

As more and more aspects of our lives depend on electronic devices and digital communication, security technologies (including encryption software) are becoming critical for matters of life and death. For example, industrial control systems and power stations need security technologies to defend them against cyberattacks that might cause them to malfunction and cause harm to the surroundings.[703] Medical devices need security technologies to prevent an attacker breaking into your pacemaker and causing it to stop.[704] Internet-connected cars need security technologies, otherwise hackers anywhere in the world might be able to take over control and cause them to crash.[705]

Cybercrime is a major worry for the future. As internet-connected devices permeate our lives and infrastructure, the risks from cybercrime are not limited to industrial espionage and fraud: lives are increasingly at stake. Engineers are already struggling to keep these systems secure, even without any deliberate weakening. Complying with the provisions of the proposed bill would only add fuel to the fire, and severely increase the risk of catastrophic future cyberattacks. Such cyberattacks may cause bigger damage than the risks of conventional terrorism and crime from which the investigatory powers are supposed to protect us.

As aforementioned examples show, digital communication systems are much more than just people talking to people; just as importantly, devices are communicating with other devices (the often-cited "Internet of Things"), and there is no clear dividing line between these different types of communication. Deliberately weakening the security of life-critical systems would not merely be foolish, but positively dangerous. Yet such deliberate weakening is precisely the effect that the Investigatory Powers Bill would have.

Signs of deliberate weakening of security technologies are also seen in the sections of the bill that deal with equipment interference (both bulk and targeted interference). A secure

---

[702] Harold Abelson, Ross Anderson, Steven M Bellovin, et al.: "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications," Massachusetts Institute of Technology Technical Report MIT-CSAIL-TR-2015-026, July 2015. http://www.cl.cam.ac.uk/~rja14/Papers/doormats.pdf

[703] "Hack attack causes 'massive damage' at steel works," BBC News, 22 December 2014. http://www.bbc.com/news/technology-30575104

[704] Marie Moe: "Unpatchable: Living with a vulnerable implanted device," Hack.lu, 21 October 2015. http://2015.hack.lu/archive/2015/2015-10-21-Keynote-Hack-lu-Marie-Moe.pdf

[705] Andy Greenberg: "Hackers remotely kill a Jeep on the highway — with me in it," Wired, 21 July 2015. http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

system is one that resists interference to the greatest possible degree; conversely, a system that permits interference must be insecure. In order to assist with equipment interference (sections 101, 116, 145 and 189), systems would have to be made deliberately insecure.

Software and mathematics do not know the difference between legitimate interference for law enforcement purposes and offensive hacking by terrorist groups and criminal gangs. It is impossible to make a system that permits legitimately and duly authorised interference, while simultaneously preventing illegitimate interference. Any "backdoor" that is put in place for legitimate law enforcement uses will inevitably be found and exploited by people who want to do us harm.

Perhaps it would be possible to rewrite the appropriate parts of the bill so as to allow law enforcement access to potential terrorist communications, while simultaneously avoiding tampering with critical infrastructure. However, this raises thorny questions of enforcement. How would one decide which communication media are legitimate targets of interception and interference, and which systems are critical infrastructure that must be as strong as possible and must not be weakened?

A major practical issue in implementing this bill is that strong encryption software is already ubiquitous. Much cryptographic software is developed as open source by communities of volunteers around the world, and made available for anyone for free. It is already built into every operating system and every web browser, and used every day by every internet user. Compelling communication service providers to assist is pointless if users apply their own encryption, leaving providers unable to comply with law enforcement orders.

The bulk collection of internet connection records is also problematic. As the recent hack of TalkTalk demonstrates, internet providers are not necessarily very good at keeping confidential customer information secure. If the internet provider is required to store details of a customer's browsing history for one year, that data may similarly be stolen by attackers, and used for blackmail or identity theft. Ironically, the government has suggested mandatory encryption of customer data to prevent this kind of attack, [706] in direct contradiction of the proposed Investigatory Powers Bill, which wants to weaken encryption.

The government has only offered weak justifications for the sweeping surveillance and equipment interference (i.e. hacking) powers of the proposed bill. Many of the arguments brought forward rely on hypothetical scenarios, and there is little evidence that the data gathered from the new surveillance powers would really help prevent terrorist attacks or fight crime. For example, the recent tragic attacks in Paris were most likely planned via unencrypted communication (which can already be trivially intercepted, without the powers conveyed by this bill) and in-person meetings (which are outside of the scope of the proposed bill).[707] Without clear evidence that the powers conveyed by the bill are necessary, it is entirely unproportionate.

[706] "TalkTalk hack: MPs to hold inquiry into cyber-attack," BBC News, 26 October 2015. http://www.bbc.com/news/business-34635583

[707] Dan Froomkin: "Signs Point to Unencrypted Communications Between Terror Suspects," The Intercept, 18 November 2015. https://theintercept.com/2015/11/18/signs-point-to-unencrypted-communications-between-terror-suspects/

Unfortunately, the security technologies that protect us from cybercrime and hostile foreign powers are the same technologies behind criminals and terrorists can potentially hide. It is not possible to take away the technologies from criminals without also removing them from the safety-critical infrastructure of our society. It is the same as with any other technology: for example, a car is mostly used by law-abiding people for legitimate travel purposes, but occasionally it may be used to transport a car bomb or escape from a crime scene. The correct response to such risks is obviously not to ban cars.

Likewise, the proposed bill is simply not an appropriate response to the threat. Instead of demonising the internet and encryption, which are mostly used for lawful purposes, a much more productive approach to preventing crime and terrorism is to use the traditional methods of policing. The cost of mass surveillance and equipment interference is huge, and the money would be much more productively spent by giving local police forces the resources to build trust with their local communities, and on diplomacy to solve the conflicts that cause radicalisation in the first place.

In summary, my biggest concern is that the current draft of the bill mandates a worrying weakening of security systems at a time when risks from cybercrime make security more important than ever. Any weakening of encryption and security systems would introduce tremendous dangers to national security, which would more than outweigh any national security benefits derived from giving law enforcement and intelligence services greater access to data.

The bill would leave citizens *less secure* than before. It disproportionately harms law-abiding citizens, by making the infrastructure on which we all rely vulnerable to cyberattacks. At the same time, it is no significant obstacle to sophisticated criminals and terrorists, who can easily find ways of circumventing surveillance and communicating securely, whether online or offline. The bill only harms the innocent, and does not hurt the guilty. It should not be passed.

18 December 2015

National Police Chiefs Council, HM Revenue and Customs, National Crime Agency—written evidence (IPB0140)

Written Evidence to the Joint Committee on the Draft Investigatory Powers Bill

Please find enclosed the law enforcement response to the call for written evidence in regards to the Draft Investigatory Powers Bill. This is a joint law enforcement response sent on behalf of the National Police Chiefs Council, HM Revenue and Customs and the National Crime Agency.

This joint law enforcement submission follows the oral evidence provided at the Joint Committee hearings on 30 November and 16 December, the Joint Committee visit to law enforcement on 15 December and provides additional detail on issues that the Joint Committee have indicated are of particular interest during these and other evidence sessions. We have not provided evidence against questions that are of no direct relevance to law enforcement, or that may have been answered by other parts of HM Government who are better placed to do so.

In summary the key points of the written evidence outlined in more detail in the submission and annexes are:

- Law enforcement welcomes the Bill. It will streamline and update the legislation for law enforcement powers in the areas of communications data, equipment interference and lawful intercept; reinforcing transparency and oversight, and protecting the public.

- The Bill will bridge the gap between the capabilities of law enforcement and criminals. Whilst criminal groups are able to take advantage of sophisticated developments in technology, law enforcement is currently unable to keep pace, match their capabilities and deliver the same criminal justice outcomes against those operating online as we are able to do in the real world.

- Law enforcement do not view the Bill proposals to changes of authorisation and oversight of these powers as an area for our comment but stress that any regime must be agile, flexible and supportive of using these powers operationally.

- Law enforcement believe concerns remain around:

    a) The definitions of the reasons for which law enforcement <u>can</u> access Internet Connection Records.
    b) Restrictions in the conduct of Equipment Interference for serious crime only.
    c) The potential for a reduction in the proposed 12 month period that data will be retained for.

- The strengthened safeguards which will improve transparency and oversight reinforcing policing by consent are welcomed.

We look forward to the Joint Committee's report being published and we would be happy to provide any further information that the Joint Committee may seek in addition to the evidence provided to date.

Keith Bristow QPM
Director General
National Crime Agency

Sir Bernard Hogan-Howe QPM MBA MA (Oxon)
Commissioner
Metropolitan Police Service

Mark Rowley QPM
Assistant Commissioner
Specialist Operations
Metropolitan Police Service

Sara Thornton CBE QPM
Chief Constable
Chair
National Police Chiefs' Council

Simon York
Director
Fraud Investigation Service
HM Revenue and Customs

Overarching/Thematic Questions:

1. **Are the powers sought necessary? Has the case been made, both for the new powers and for the restated and clarified existing powers? Are the powers sought legal? Are the powers compatible with the Human Rights Act and the ECHR? Is the requirement that they be exercised only when necessary and proportionate fully addressed?**

    a. Law Enforcement (LE) believe that the powers are absolutely necessary as a part of the overall mix of capabilities they require for protecting the public. The powers considered in the draft Investigatory Powers Bill (IPB) streamline and update the legislation in the areas of Communications Data (CD), Lawful Interception (LI) and Equipment Interference (EI), ensuring that they address privacy concerns and provide a more transparent regime with rigorous oversight. The powers are all vital tools required to bridge the gap that is developing between criminal use of technology and LE's ability to operate effectively in this dynamic digital environment. Additional detail on the changing technological landscape is provided in **Annex A**.

    b. LE do not consider that the IPB introduces any 'new' powers. Instead it enables existing capabilities to be maintained in the digital environment. The LE requirement for CD has been consistent for many years; the crime types that are

investigated have changed little though technology has enabled criminals to develop old crimes in new ways, and made certain types of crime more accessible; the technology that supports those that wish the public harm has changed, and now includes the rise of cyber-enabled and cyber crime. The only change introduced in the IPB is the requirement for Communication Service Providers (CSPs) to retain more information on their customers' use of their services (Internet Connection Records (ICR)) and provides a statutory footing for LE to request this data under specific, targeted circumstances. Additional detail on what an ICR might look like is provided in **Annex B**.

c. LE act in accordance with the law and existing processes already ensure that the activities which are the subject of the IPB always consider the implications and impact of the Human Rights Act[708] and the ECHR whatever activity they are considering and whatever power that they might use. On every occasion, necessity, proportionality and collateral intrusion, where it might occur, are considered during each stage of the application and authorisation process.

d. It should be remembered that LE work is evidential, which is different in many respects from the Security and Intelligence Agencies (SIAs), and it is targeted. Unlike the SIAs our work is often subject to the test of scrutiny in a court and is subject to external, rigorous oversight and disclosure. The capabilities LE use are brought to protect the public but also to bring people to justice and to discount people and prove alibis.

2. Are the powers sought workable and carefully defined?

a. LE believe they are; there remain areas where LE expect clarification to be provided on how the powers will work in practice but believe a practical and technical solution could be implemented in order to deliver the capabilities LE need.

General Questions:

3. Are there any additional investigatory powers that security and intelligence services or law enforcement agencies should have which are not included in the draft Bill?

a. LE identified five core operational requirements for CD which were articulated during the review of powers by David Anderson QC, and set out in his report 'A Question of Trust'. These are to:

- **i.** Link an individual to an account or an action
- **ii.** Establish a person's whereabouts
- **iii.** Establish how suspects or victims are communicating
- **iv.** Observe online criminality, and
- **v.** Exploit data [to corroborate evidence, identify further investigative leads]

b. These remain LE requirements for investigations. Under current legislative provisions, particularly for CD, LE is increasingly unable to meet these five requirements when a suspect or victim's activity takes place online. The IPB goes

[708] For example, LE often has to balance a matrix of qualified rights such as privacy and freedom of thought, expression, and non-discrimination with that to save life and protection of persons and fair investigation and trial.

a long way to meeting these requirements, but a restriction has been placed in the IPB in respect of exploitation of ICRs that will significantly reduce investigative capabilities.

c. S.47 imposes restrictions on the granting of authorisations, limiting the purpose for which ICRs can be obtained to identifying - who has used an internet service, where the service and time of use are known (Internet Protocol Address Resolution (IPAR)); which Communications Services a known individual has used and where or when a known person has accessed illegal material. These provisions significantly restrict the opportunities that an investigator may develop from the information derived from ICR's and mean that not all five LE requirements can be met. There are a number of examples in **Annex D** that draw this point out.

d. In essence, and in both proactive and reactive investigations, if LE are denied the opportunity to derive information from ICRs that are not those set out in s.47, for example information pertaining to such activities as using a travel webpage, a banking service, a car rental company, or making online purchases, then investigative opportunities are unknown and investigations may cease altogether. This is because it will be very rare for any other opportunities to exist. This pursuit of different lines of enquiry is normal tradecraft for most investigators, whether it be for a missing person or the understanding of conspiracy by an organised crime gang. This problem does not/did not occur where traditional telephony is used and call records indicate that a voice call took place but with the advent of voice being made into data travelling from one IP address to another, then ICRs are vital for LE to retain the capability to pursue enquiry opportunities.

e. If it is assumed that ICRs are to provide LE with avenues for investigation, where those avenues cannot be explored due to jurisdictional limitations, the IPB makes no provision for alternative approaches (for example under Mutual Legal Assistance). This is particularly relevant to overseas service providers in jurisdictions where UK LE have no legal recourse and where it is unlikely there might be any formal or informal cooperation. This issue may have been addressed under the third party provisions, but there is no requirement placed in the IPB for the retention of third party data that does not originate or terminate on a UK CSP's network.

f. In a separate issue, s.46 sets out the purposes in which a designated senior officer may authorise access to CD. These are comprehensive but LE is concerned in respect of the wording in s.46 (7) (g) which allows for CD to be obtained, where necessary and proportionate, for the purpose of preventing death, injury or damage to a person's physical or mental health – in an emergency. It is within this 'emergency' category where there may be potential difficulties. Hundreds of people are reported as missing in the UK every year, many of them are classed as vulnerable due to their age or mental or physical health and LE would rightly seek to limit the danger to which such individuals are exposed by locating them as soon as reasonably practicable. Not all instances would be deemed an 'emergency' and it is unclear why CD cannot be used as a tool of early

consideration rather than meeting the requirements of last resort to prevent harm to an individual. LE believes that 'saving life' should be explicitly available as a justification to avoid emergency situations. LE believe that the term 'emergency' should be referenced as being for civil contingencies such as kinetic transport disasters; rail or air crashes or terrorist incidents where the identification of people for emergency response will be required by LE as the lead for public authorities.

g. Finally, the practical implementation of the provisions of the IPB, by LE and by industry, may take time to be fully effective, and so there will remain gaps in LE investigative capabilities until full implementation is achieved.

4. Are the new offences proposed in the draft Bill necessary? Are the suggested punishments appropriate?

a. LE do not believe it is necessary to introduce additional offences above those that already exist in legislation or in common law (for example Misconduct in Public Office) which already cover the proposed offences outlined in the Draft Bill.
b. In particular, the concept of 'reckless' proposed in the Draft Bill, whether this may be clarified in any Code of Practice, does not make it clear what the offence is attempting to cover when no offence is committed if the CD is obtained under an authorisation.
c. Subject to the requirements of Parliament, should such an offence be deemed necessary, then 'reckless' could be more appropriately replaced so that an offence is only committed when a person intends to acquire CD without an authorisation. This is consistent with the offence in s.2 which provides that an offence is committed if there is intentional (not reckless) interception.

Interception Questions:

5. Are there sufficient operational justifications for undertaking (a) targeted and (b) bulk interception?

a. The IPB does not permit LE to conduct 'bulk' interception. All LE lawful interception (LI) is tightly targeted and provides LE with significant operational benefits. It is used as a source of intelligence which assists in identifying and disrupting threats from terrorism and serious crime. It supports the gathering of evidence and identification of opportunities, where it meets the necessity and proportionality thresholds, eg. to tackle the supply of prohibited drugs, people trafficking, fraud, child sexual exploitation, firearms and the proceeds of crime. The importance and dependence on the intelligence provided through targeted LI is likely to remain of vital importance.
b. **In the broader LE context, but very specific to how targeted LI is used by HMRC, the following illustrates how important such capability is:**
    i. **HMRC faces a number of key organised crime threats including cigarette and tobacco smuggling; alcohol smuggling and diversion; the smuggling and laundering of oils; VAT multi trader intra community (MTIC) fraud;**

and non MTIC attacks on HMRC repayment systems including Self-Assessment, VAT and Gift Aid.

ii. **Targeted interception is a key capability which provides HMRC with the intelligence to support operational activity which leads directly to arrests, seizures (of contraband, criminal assets and money) and prosecutions. But it also makes a significant contribution to HMRC's strategies to counter organised attacks on its systems. Interception can provide a clear understanding of criminal techniques and strategies. This intelligence is used to drive changes in policy, processes and legislation to strengthen any weaknesses in HMRC's systems that crime groups may seek to exploit. Interception is an agile tool that can keep pace with the speed with which crime groups adapt to changes in HMRC's control methods. In 2014/15 targeted interception and communications data supported investigations that prevented just over £2 billion in revenue loss.**

6. Are the proposed authorisation processes for such interception activities appropriate? Is the proposed process for authorising urgent warrants workable?

a. LE consider that the proposed authorisation for a 'double lock' process, where it provides additional oversight and transparency by a Judicial Commissioner can be supported, subject to there being no impact on the current regime of flexibility and agility of response in a dynamic 24/7 environment.

b. LE is concerned that the urgent out of hours authorisation process for modifications to a Warrant has been adversely impacted by the proposed increase in grade/rank for such authorisations. The limited availability of such senior officers risks creating delays in operations given that they also have limited time available to make authorisations. This could, perversely, lead to a reduction in safeguards with senior officers taking less time to examine applications. LE would seek to use the current process whereby a suitably trained, experienced and accredited Superintendent may authorise a modification in such circumstances.

Communications Data Questions:

7. How well does the current process under Mutual Legal Assistance Treaties (MLATs) work for the acquisition of communications data? What will be the effect of the extra-territorial application of the provisions on communications data in the draft Bill?

a. Mutual Legal Assistance is the formal way in which countries request and provide assistance in obtaining evidence located in one country to assist in criminal investigation or proceedings in another country. Mutual Assistance in Criminal Matters between the Member States of the European Union supports the exchange of information and includes a section on requests for communications data that are routed through the relevant Central Authority. In light of the significant proportion of communications providers based in the United States of America, there is a Mutual Legal Assistance Treaty between the UK and the USA.

b. The process for LE acquisition for CD through the MLAT process, involves meeting the administrative and judicial standards for evidence (or relevant request) in the requesting country, passing the request to a Central Authority that checks the request for compliance with national MLA legislation and the relevant treaties, and then passes this to the receiving country's Central Authority, who also check for compliance with their national MLA, relevant treaties and the national legislation governing the request. The receiving Central Authority will then pass it to a national authority who can turn the international request into a national request under the receiving country's legislation and national administrative processes. This may include, as it can in the USA, making a request to a court for a relevant warrant or order and then this being passed to law enforcement to serve on a company. Unless any of the individuals' or authorities' sole focus is on international cooperation - like the Central Authority, or some specialist departments in US District Attorney's Offices - carrying out the administrative process for a foreign country is likely to be a task added onto their normal workload. In addition to this, the request is likely to be written to fulfill the requesting country's administrative and legal practices, not in those of the receiving country's. This includes omitting specialist language that particular requests may require.

c. The current process may take several weeks, or even months and there is therefore no guarantee that requests will meet with deadlines for trial. Work is underway however to streamline the processes, including moving several of the stages from 'hard copy' on to an electronic system. Despite these improvements, Mutual Legal Assistance is not a substitute for obtaining data under the IPB as, given the inevitable time-constraints in the process, MLAT does not support agile intelligence development during a criminal investigation. All reasonable steps have been taken to improve the process over the past two years, including comprehensive training and awareness programmes initiated to enhance awareness of investigators and prosecutors for the early identification of MLAT opportunities. Whilst the quality of the data returned will continue to meet LE requirements, this streamlining will significantly improve how well the current process functions. LE recognises the efforts in this area but would welcome any further legal provisions which could assist in achieving faster and more agile responses.

d. UK law is clear that companies providing communications services to users in the UK, irrespective of where they are based in the world, must comply with lawful requests from the UK authorities. The UK Government intends to maintain these obligations in the IPB. We expect any multinational firms operating in any industry in the UK to act in accordance with our laws and we have always sought to work with companies to this end.

8. Does the draft Bill allow the appropriate organisations, and people within those organisations, access to communications data?

a. Please see our response to Q3 above.

b. CD is regularly used as evidence in criminal prosecutions. Largely, the data entering the criminal justice system comes from data retained under legislation. CD provides vital evidence of:

- **i.** Chronology (the time and sequence of events in relation to a particular case – CD is more reliable than witness memory of events, for example);
- **ii.** Association (victim with witnesses or suspects, suspects with one another);
- **iii.** Presence or otherwise in a geographical locus (not necessarily at a particular location – can also be vital, in certain circumstances, from a defendant's perspective);
- **iv.** Corroboration (of other evidence in the case and in particular of the testimony of criminal or vulnerable witnesses).

9. Is the authorisation process for accessing communications data appropriate?

a. LE believe that the current process is appropriate: It is explained in diagrammatic form at **Annex C**, and was commended in the Report of the Draft Communications Data Bill (2013) and by European Commissioners during their review of the Data Retention Directive (2014).

10. Is accessing Internet Connection Records essential for the purposes of IP resolution and identifying of persons of interest? Are there alternative mechanisms? Are the proposed safeguards on accessing Internet Connection Records data appropriate?

a. The information provided below is in addition to the explanation above and that contained in the ICR annex.

b. IP addresses are a fundamental requirement to enable devices to communicate over the internet. Due to a shortage of IP addresses, however, CSPs have to share single IP addresses across several thousand users in any one instant. There is often a requirement, as part of an investigation, to identify who was accessing a service from a known IP address at a particular time. The challenge of mapping use of a single IP address back to a single user is further exacerbated due to discrepancies between server times across the world. This results in law enforcement having to allow a margin of error, in terms of seconds or minutes, when seeking resolution.

c. Given that in any one instant there may be several thousand users on the same IP address the inclusion of the relevant port number, even were it available in most investigations, (which it is not), – does not sufficiently refine the search to enable accurate resolution. In the time window LE may have to provide there may be several people allocated the same IP address and same port number.

d. If LE could structure their query in terms of- who was using this IP address (and this port number if available) and using this specified service, the resultant response would be as refined as is technically possible, thereby reducing collateral intrusion to an absolute minimum. LE will frequently know the relevant service, whether it is an event conducted through for example. Hotmail, Facebook or Twitter, and could provide this as part of the query. Previously there

was little point in providing this additional detail because CSPs had no way of tailoring the query of their system to this level. In order to do so they would require collection of ICRs.

e. The Counter Terrorism and Security Act 2015 (CTSA) provisions were intended to provide LE with the ability to resolve an IP address to an individual through the resolution of an IP address to a person or device. The provisions under CTSA did not however, permit the destination IP address or service name to be stored, therefore IP Address Resolution (IPAR) would not resolve to an individual in the majority of cases. Following Royal Assent for CTSA, LE has worked with the Home Office to determine how IPAR could be implemented and to determine what data would be required to be retained by the UK CSP. We established that in order to resolve an IP address to an individual, specific data needs to be retained which goes further than that specified in CTSA. The additional data required to be stored is the source IP address, the source port number, the destination IP address (or service name). It is this record, coupled with data and time information, that allows the reduction of the number of individuals to which the information will resolve to. This is why full ICR retention is imperative to the ability to enable IP address resolution for retrospective investigations.

Equipment Interference Questions:

11. Should the security and intelligence services have access to powers to undertake (a) targeted and (b) bulk equipment interference? Should law enforcement also have access to such powers?

a. The IPB provides the ability for LE to authorise and undertake targeted equipment interference (EI). LE will not have access to bulk EI powers.

b. EI is currently authorised and conducted by LE under the Police Act 1997 (together with other authorisations as appropriate, including RIPA surveillance authorisations). The IPB consolidates this existing legislation and sets out a clear framework for the authorisation of equipment interference.

c. LE currently use a variety of EI techniques to prevent and detect serious crime. These different techniques range in sensitivity, complexity and intrusiveness and are deployed in a targeted and proportionate way. At the more intrusive end of the spectrum EI could be used by LE as part of a proactive investigation, for example to retrieve data from a criminal's electronic device for use in evidence. At the less intrusive end, EI could be used by LE to acquire specific data for intelligence only purposes (such as to identify the methods of communication used by an organised crime group to conduct their criminal activities). Equally, EI is a crucial tool in responding to emergency situations, such as a kidnap, where the ability to quickly use these techniques can be the difference between life and death.

d. EI already provides significant operational benefit to LE by facilitating the obtaining of information and evidence that can not be captured by other means – for example where encryption technology is being used to hide criminal communications. However, as technology develops and criminals become ever

more sophisticated with it, EI will become an increasingly crucial tool for LE in maintaining its ability to effectively prevent and detect serious crime.

e. *LE also considers EI techniques to be essential for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health. The IPB currently makes no provision for authorising EI for this purpose, and LE consider it should be included.*

f. It is understood that the Home Office intends to limit, in the Codes of Practice, access to the more advanced and intrusive techniques to specialist units within LE. This approach will assist in ensuring that EI techniques are deployed proportionately and by those with relevant expertise.

12. Are the authorisation processes for such equipment interference activities appropriate?

a. The authorisation process requires all EI warrants be issued by a law enforcement chief and approved by a Judicial Commissioner. This will ensure detailed scrutiny and independent consideration of all EI warrants.

13. Are the safeguards for such activities sufficient?

a. LE recognise the responsibilities and obligations placed upon it by the safeguards provided for in the IPB and agree that these are necessary to protect the interests of those whose data is obtained under an EI warrant.
b. Accordingly, LE will put in place arrangements for ensuring material obtained under an EI warrant is held securely and handled appropriately. Importantly, the safeguards recognise that material obtained under an EI warrant can be used in evidence and, in appropriate circumstances, it will be necessary to disclose this material. Accordingly, the provisions provide for arrangements to be put in place that take into account the use of material in legal proceedings and the performance of the functions of LE agencies.
c. LE also recognises the importance of preserving the evidential integrity of equipment that has been the subject of EI. This will continue under the IPB and LE will work closely with prosecutors to ensure the fairness of any prosecution.

Additional Matters:

14. Retention Periods

a. Considerable detail was captured during an ACPO Data Communications Group evidence capture exercise during a two week period in 2012. The data and evidence from that report is provided at **Annex E**.

b. In a recent Child Sexual Exploitation (CSE) major operation, where Communications Data played almost the sole route for supporting the investigation, the NCA was able to deal with 92% of the requests for CD. The remaining 8% were already more than 12 months old and for which no data

would have been retained. If reduced periods were imposed on this particular operation, then it would have had the following effect:

i. Period reduced to 9 months – 66% potentially resolvable
ii. Period reduced to 6 months – 39% potentially resolvable
iii. Period reduced to 3 months – 13% potentially resolvable.

c. So if retention periods are reduced, and particularly for this crime type, it is unlikely that the NCA could have carried out such an operation, with the commensurate loss of opportunities to identify serious offenders and protect or safeguard children at risk of or suffering abuse.

15. Protective Security

a. Law Enforcement rely on a number of Government mandated standards for managing protective security. They are designed to be implemented to mitigate identified and assessed risks. The baseline for protective security is founded upon:

i. Personnel Security: Due diligence followed by an enhanced national security vetting is conducted to ensure that law enforcement officers and staff maintain a level of integrity, honesty and trustworthiness that is commensurate with the information they can access. These processes are additionally supported by a comprehensive vetting aftercare process, to manage changes in circumstances and risks.
ii. Physical Security: Both physical and procedural security measures are deployed, such as robust building design, locks, alarms and auditable access control systems to protect law enforcement activity and data from unauthorised access.
iii. Information Security: Confidentiality, Integrity and Availability of data is assessed and proportionate protection, auditable access control, and secure data storage are implemented to prevent unauthorised access. This is additionally enhanced with a proportionately robust audit process.
iv. Training: All officers and staff that are involved in the processing of applications for investigative powers undergo mandated training relevant for the role; for example the Single Points of Contact (staff with responsibility for acquiring the data from a CSP) undergo formal and continual assessment before they can be issued with a "Personal Identification Number" that grants them access to a CSP's data.

Annexes:

A. Technology and the Impact on Investigations (Q1).
B. IPB Provisions for CD (Internet Connection Records) (Q1).
C. Authorisation Process for Accessing CD (Q9).
D. Threat Picture Operational Examples (Impact of the CD clauses of the IPB) (Q3).
E. 2012 SPOC Survey (Q14).

Annex A - TECHNOLOGY AND THE IMPACT ON INVESTIGATIONS

The internet has revolutionised communications

The infrastructure over which communications are transmitted has fundamentally changed with the development, and increased use of the internet. In turn the devices and way in which we access and interact on the internet has changed.

When the Regulation of Investigatory Powers Act 2000 (RIPA) was written a mobile phone could only be used for phone calls and text message. Today we are able to access the entire internet from our phones and mobile devices which means we use them for many more things at home and on the move from; emailing, browsing the internet, online banking, location services, directions, social networking, reading and listening to music.

Our style of communication has also moved from person to person to social media, broadcasting messages to groups of people that are likely to have never met or ever intend to meet.

- In 2015 the average adult spends 2.5hrs a week online on the move (five times that of 2005).
- Instant messaging use has increased from 38% in 2013 to 42% in 2014 driven by services such as Facebook messenger and WhatsApp.
- Social media is used by 80% of internet users aged between 35 and 44 compared with 12% in 2007.

Increasingly, the use of 'traditional' communications is becoming outdated. Landline phone numbers are decreasing as people opt for more convenient methods of communication.

Impact of Internet based Communications on Investigations

The rapid change of global communications technology introduces a digital challenge to Law Enforcement.

The internet has transformed the way in which people communicate. The nature of the internet means that there are no borders and as such the use of the internet for crime is a global problem and ultimately needs a global solution. Individuals are able to contact people all over the world in milliseconds, for no additional cost on multiple platforms. This advantage also extends to criminal use where connections are made where they wouldn't have been before. It also means that services are provided to UK customers from all over the world. The services cited as the most used by internet users such as Microsoft, Google, Facebook etc are predominantly based in the US creating challenges between domestic and international legislation.

Whilst these services are legitimate they are frequently used by criminals to facilitate crime which was not foreseen in the creation of these capabilities and creates competing demands on these companies and their duty to shareholders and customers.

The internet facilitates actions of those wishing to cause harm to the public and provides a degree of anonymity in doing so. The internet enables crime to be carried out on an industrial scale from online fraud to the sharing and distribution of child abuse images. New criminal activities have also been created with the advent of the internet such as the hacking of personal data which is held to ransom.

Whilst criminals become more adept at using the internet to facilitate crime, the capability that Law Enforcement (LE) has under current legislation has degraded since it does not enable powers of investigation to keep pace with the change in technology.

The change in technology, how people interact on and connect to the internet has also affected what information and intelligence Law Enforcement Agencies (LEA) are able to gather in the course of investigations. With the correct and appropriate access to this information LEA would be able to improve profiling and understanding of a suspect or victims' movements, contacts and actions both proactively and reactively. Arguably, making investigations more efficient and timely.

Traditional and Digital Communications Data Explained

Traditional Communications Data

Traditionally, communications over landlines and mobile networks meant that Communication Service Providers (CSPs) kept records of who spoke to who, how, when and where they were. A large portion of this information would be found on an individual's phone bill.

Figure 1: Example of Communications Data held under RIPA 2000

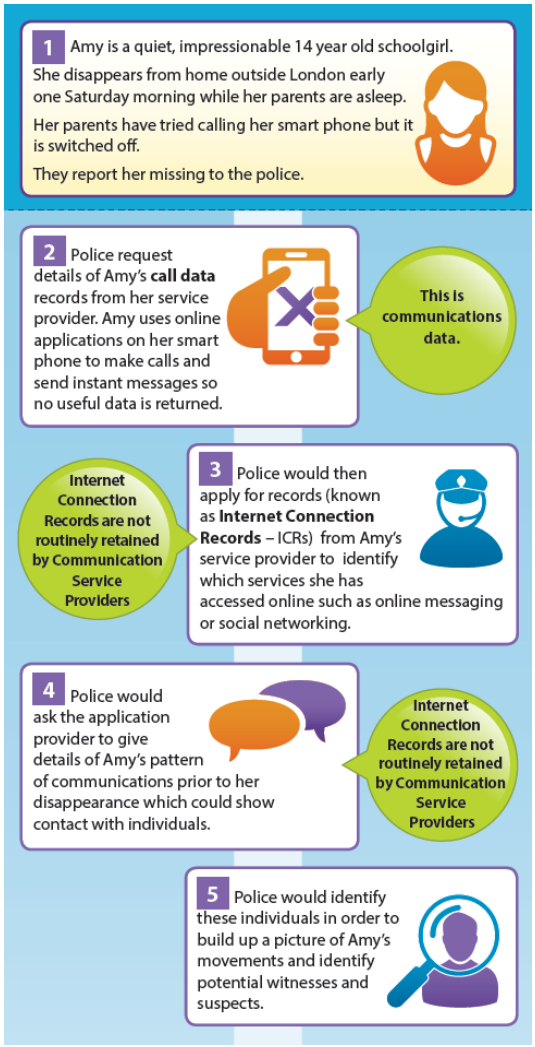
Date	Time	Type	Duration	A Party	B Party	IMEI	Site	Postcode	Last Cell
03-Oct-14	18:37:07	Mobile	00:00:44	7777111111	7787444444	3562870570	Hammersmith	W12 0HS	W12 0HS
03-Oct-14	18:52:10	Mobile	00:05:52	7777111111	7553662445	3562870570	Hammersmith	W12 0HS	W12 0HS
03-Oct-14	19:12:46	Mobile	00:01:19	7777111111	7787444444	3562870570	Hammersmith	W12 0HS	W12 0HS
03-Oct-14	20:22:35	Mobile	00:00:18	7777111111	7957776614	3562870570	Hammersmith	W12 0HS	W12 0HS

WHEN HOW WHO WHERE

This data is available to LEAs subject to RIPA 2000 authorisations and is still used in almost all cases by LEAs since it will often provide either a crucial starting point for an investigation or support leads of enquiry. RIPA means that UK CSPs have to retain details of their customers communications for 12 months, if it is not requested by LEAs within this time period it is automatically deleted.

A 12 month retention period is important because it is often unknown that a criminal act will take place. As such data must be stored proactively to allow for re-active investigations. (Further information on retention periods is available in **Annex E**.)

Figure 2: Use of Communications Data from 'traditional' communications



Digital Communications Data

Current legislation and access to this data has not kept pace with 21st Century capabilities and LEAs are increasingly blind to criminal communications and actions online.
Securing the equivalent of communications data online to that which is currently held offline takes LEA a step towards gaining back the ground that has been lost in the digital world between LE and criminal activity online, or facilitated by the internet.

Law Enforcement can not currently consistently access CD from online communications because not enough data is routinely stored by service providers. CSPs do not record the same type of information for online based communication as they do for traditional telephony. CSP business models are concerned with the amount of data their customers are using rather than the individual records of phone calls, texts and services accessed online. They retain data that is useful for billing, marketing and identifying trends of use across their customers rather than details of individual customer use.

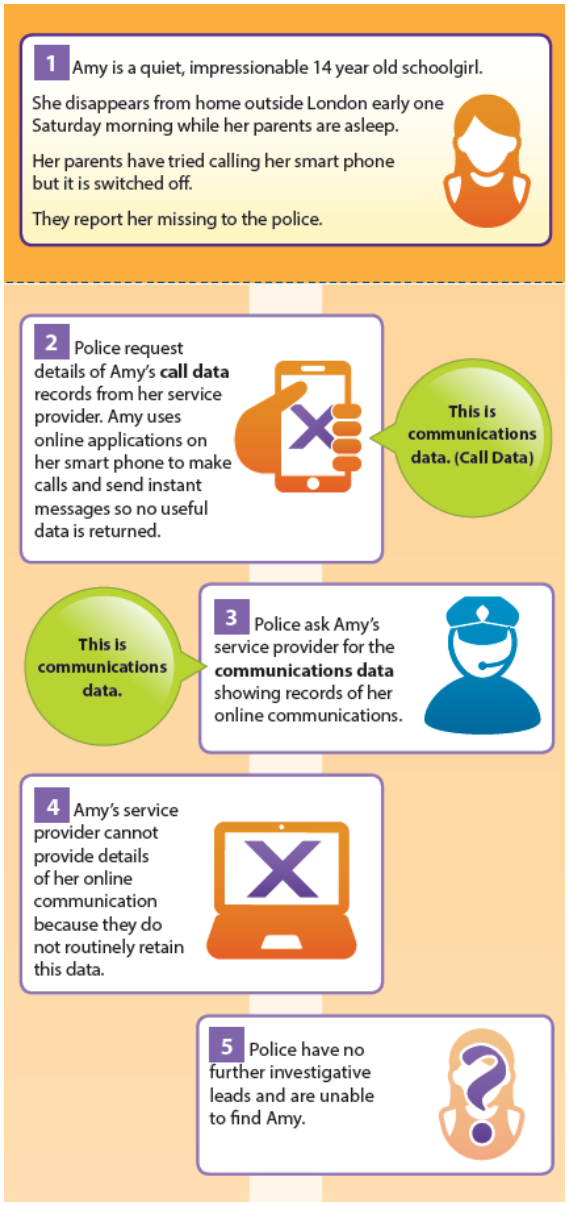
To maintain the LEAs' needs, the require to have better access to online CD, and current provisions do not meet the LE requirement to effectively investigate criminal activity when it is facilitated by online services.

Figure 3: Example of Communications Data held by CSPs for internet based communications

Date	Time	A	IP Address	Access point	Duration	Data upload	Data Download	IMEI	Site postcode	Bearer
03-Oct-14	18:37:07	7777111111	10.186.133.222	MobileTel	00:06:19	41705	230	3562870570	W12 0HS	3
03-Oct-14	18:52:10	7777111111	10.95.236.113	MobileTel	00:00:12	2182	7919	3562870570	W12 0HS	3
03-Oct-14	19:12:46	7777111111	10.58.134.140	MobileTel	00:06:31	1162	184	3562870570	W12 0HS	3
03-Oct-14	20:22:35	7777111111	10.42.165.73	MobileTel	00:07:48	6761	179800	3562870570	W12 0HS	3

WHEN **WHERE**

Figure 4: Example of the current capability to access online Communications Data



Improvements Law Enforcement need to online Communications Data

Internet Protocol Address Resolution (IPAR) is used to link an individual or account to an action online.

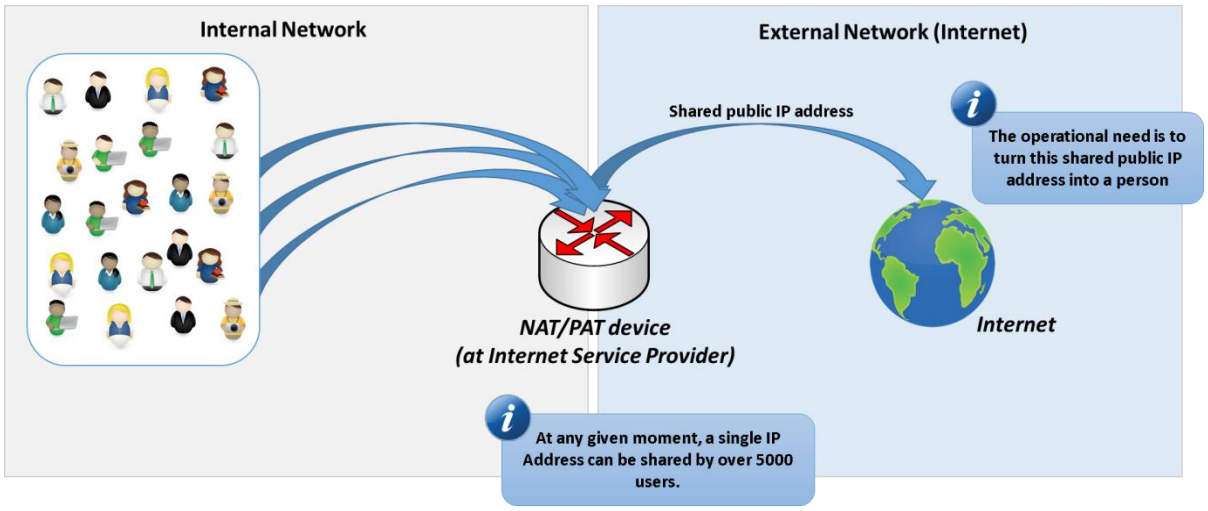
IPAR is increasingly challenging due to the amount of information that is passed over the internet and the Internet Protocol (IP) used to link devices / actions to individuals.

An IP address is the unique number assigned to every device on the internet. The IP address is akin to a phone number in traditional CD or a postal address that identifies where a letter is destined for.

The growth of the internet means that since the 1980s predications have been made that the original 4.3billion IPv4[709] addresses would be exhausted. This finally happened in 2011 and was mitigated to some extent by changes in the IP address allocation and routing infrastructure of the internet.

The process of NAT (Network Address Translation) and Port Address Translation (PAT) which enables service providers to manage the limited number of IP addresses available more efficiently makes IP Address Resolution (IPAR) difficult since IP addresses are shared. One 'public' IP can be used by many thousands of 'private' users making it impossible for an action online to be linked back to a specific device without further identifying information.

Figure 5: The NATPAT Problem



The problem of resolving IPs is exacerbated by the fact that servers across the world are not synchronised in terms of timestamp. An IP address with a date and timestamp to the tenth second captured for example by Facebook may be seconds out from the timestamp used by Vodafone in the UK whose service is used to access the site. To allow for this difference, search terms are widened by a few seconds either side of the Facebook timestamp and as such the search term can return tens of thousands results.

The Counter Terrorism and Security Act 2015 (CTSA) intended to make it possible for LEAs to resolve IP addresses: engagement with CSPs and technology companies has identified that insufficient information is retained to enable IP addresses to be resolved in all situations, particularly on mobile internet access.

[709] Internet Protocol version 4

Without additional information about these communications over the internet, LEA are unable link a device to actions online and identify crucial information for investigations.

Annex B - BILL PROVISIONS FOR COMMUNICATIONS DATA

Internet Connection Records Explained

The Bill introduces Internet Connection Records (ICRs) as a term for the data which details the connections made from a device across the internet to other online services. These ICRs will record the following information:

1. The time of the connection – providing the **when**
2. The location of the device making the connection – providing the **where**
3. The service(s) the device was accessing – providing the **how** but **not what** was done on that service.
4. The identity of the device – that can lead to understanding the **who**

Yet to be defined, the additional data an ICR could include port numbers, destination IP addresses, time and service or host name.

Figure 6: Example of what an Internet Connection Record could look like

Date	Time	MSISDN	Source IP	Source Port	Dest. IP	Dest .Port	Service / Domain	Post Code
07/10/15	09:17:26	07771966917	234:96:17:113	2237	141.92.130.226	443	**Lloyds Bank**	W12 0HS
07/10/15	09:18:37	07771966917	234:96:17:107	61123	213.174.196.17	80	**Easyjet**	W12 0HS
07/10/15	09:19:15	07771966917	234:96:17:119	8987	238.226.19.35	5222	**WhatsApp**	W12 0HS
07/10/15	09:19:55	07771966917	234:96:17:119	1592	50.31.0.12	80	**Maplin Electronics**	W12 0HS
07/10/15	09:21:34	07771966917	234:96:17:109	35227	23.218.220.133	80	**Marks and Spencer**	W12 0HS
07/10/15	09:22:19	07771966917	234:96:17:102	26559	94.245.104.73	80	**NHS**	W12 0HS

WHEN

WHO 'A'

HOW

WHO 'B'

WHERE

This information would never provide a full web browsing history of a suspect or victim. Nor would it ever provide the content of communications but as with traditional CD, would provide a starting point for further targeted lines of enquiry.

As with traditional CD, this data needs to be proactively retained since it is mostly unknown that a criminal act will take place. A large proportion of investigations carried out by LE are reactive, only starting once an alleged crime has been committed.

Draft Bill provisions for Law Enforcement

As stated in David Anderson's review 'a question of trust' the Law Enforcement requirement for Communications Data are to:

1. Link an individual to an account or an action
2. Establish a person's whereabouts
3. Establish how suspects or victims are communicating
4. Observe online criminality, and
5. Exploit data [to corroborate evidence, identify further investigative leads]

Clause 47 in the draft Investigatory Powers Bill enables the retention and restricted access (by Law Enforcement) to Internet Connection Records (ICRs) for the purposes of;

- identifying the sender of a communication (LE requirement 1&2),
- identifying the communication service a person is using (LE requirement 3), and
- determining whether a person has been accessing or making available illegal material online (LE requirement 4).

These provisions meet four of the five Law Enforcement requirements and are very welcome but there will remain crucial gaps in LE capabilities which restricts our ability to discharge our responsibility to protect the public.

The fifth LE requirement is crucial to investigations; often a suspect or victim is known and the investigative query is based on understanding their actions to enable further follow up lines of enquiry.

Access to ICRs to understand their digital footprint would provide investigative leads in the digital and real world. Restricting LEA from requesting this type of data significantly hinders the capability for LE to protect the public.

The limitations mean that although the data is retained, LEA will be unable to request all data concerned with an investigation. There could be further evidence that can identify or exonerate a suspect and/or locate a missing person that exists but which cannot be requested by Law Enforcement under the IP Bill provisions.

Law Enforcement remain concerned that such a restriction is incompatible with their ability to protect the public, or seek to bring about a fair trial.

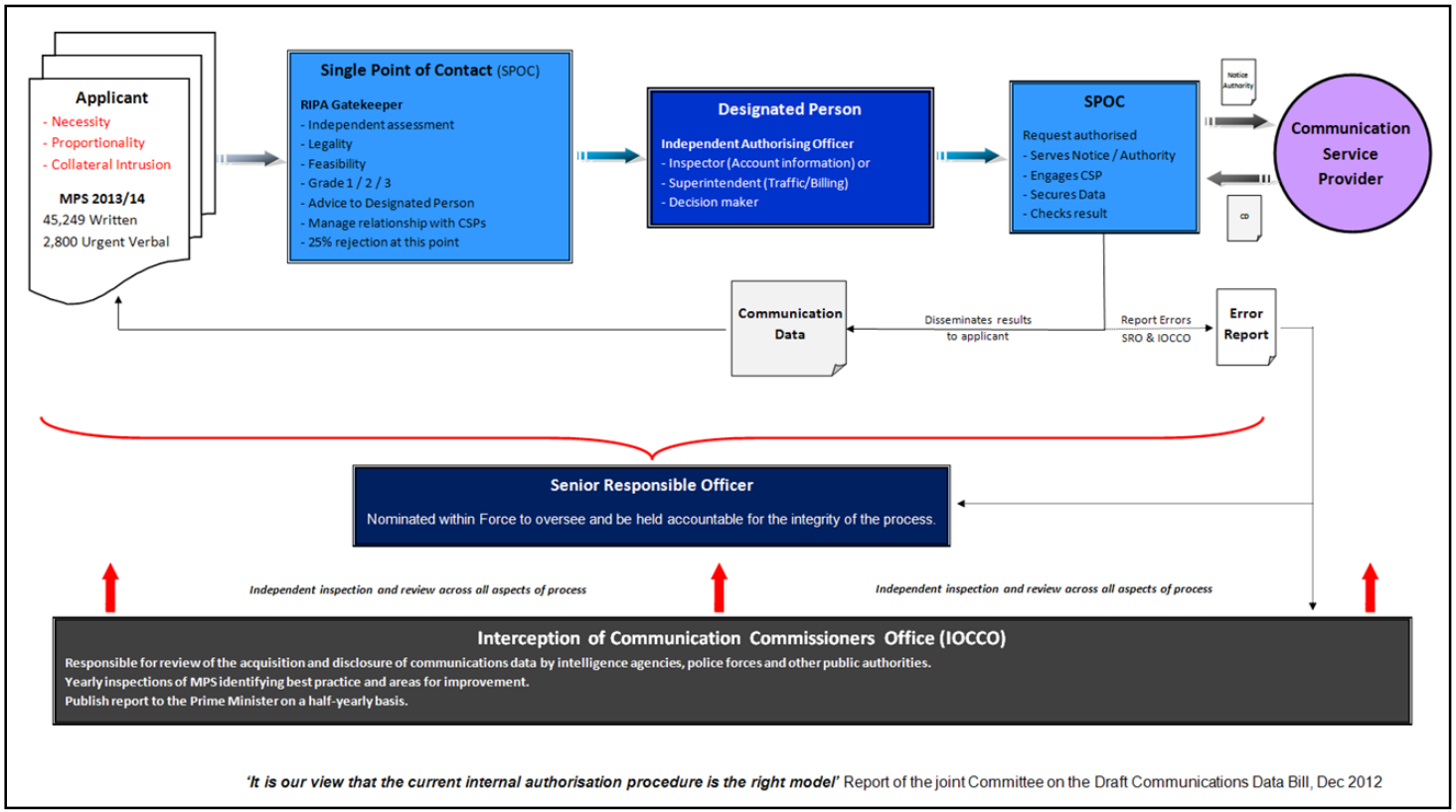
In seeking the authorisation of a request for communications data the applicant must demonstrate that the request is for a statutory purpose, typically for the prevention and detection of serious crime. As such, all applications are targeted towards those suspects or victims that are believed to be engaged in serious criminality or are at risk. Intelligence and

evidence gathered through the analysis of Communications Data therefore enables investigators to identify the actions of the suspect or victim within appropriate timescales and will be crucial to progress investigations.

When individuals use 'traditional' calls and texts no differentiation is made between the types of services accessed and data returned to Law Enforcement. There are hundreds of cases across all areas of serious crime where this information is important to investigations however the provisions of the draft IP Bill place restrictions on the access and use of this data when it is online.

Annex D sets out the sort of challenges faced in day to day policing and investigation of serious crime related to for example missing persons, children and vulnerable people when the internet is used as a means of communication and access point to services that would otherwise have been made in the 'real world'. An assessment of how the draft IP Bill would impact these types of investigations has also been included as currently understood. A summary is included that shows the impact on proactive and reactive enquiries where law enforcement seek to exploit Communications Data not linked to either a Communications Service or accessing illegal material. This might include where details of planned travel, banking, and some online purchases (relevant to a crime but the possession of which would not of itself amount to a crime) all of which would establish a pattern of behaviour leading to a number of other enquiries. This is normal procedure for most investigations whether for a missing person or investigation into a crime where there might be a number of suspects.

Annex C – Authorisation Process for Accessing CD



Applicant A person linked to or the Investigator of a criminal offence, normally a Constable or member of Police Staff, who require Communications Data in order to complete investigations. They consider and record the elements of **necessity**, **proportionality** and **collateral intrusion**. Although necessity is an objective test, applicants are required to articulate how the application links to the crime or the individual concerned.

Single Point of Contact (SPoC) Accredited Individuals trained as guardians and gatekeepers for the process. The SPoC is independent of the investigation and dedicated to the process, they provide advice to the operation and also act as a focal point for Communication Providers. SPOCs grade the response according to threat - G1 (Immediate Threat to life), G2 (exceptionally urgent operational requirement, serious crime) and G3 (routine).

Designated Person Senior officer at a rank stipulated by Parliament, trained to consider the impact on human rights of acquisition. This individual must be independent from the investigation and considers both the application and advice from the SPoC to a standard that will withstand scrutiny.

Senior Responsible Officer (SRO) The process is overseen by the nominated SRO who is held accountable for the integrity of the process,

Interception of Communication Commissioners (IOCCO) Independent oversight body – independent of Government and Parliament - reviews the interception of communications and the acquisition and disclosure of communications data by intelligence agencies, police forces and other public authorities by conducting yearly inspections. Produces report to Prime Minister on a half-yearly basis.

Annex D - Threat Picture Operational Examples: Impact of the Communications Data clauses of the Investigatory Powers Bill

Crime: Child Sexual Exploitation and Abuse (CSEA)

CSEA remains a particularly significant threat, with every UK policing region reporting cases of contact child sexual abuse (CCSA) in 2014; the proliferation of indecent images of children (IIOC) and online child exploitation (OCSE) continue to subject children to risk.

Impact of the Internet: The current volume of referrals to the NCA of UK-based individuals sharing indecent images of children (IIOC) online, approximately 1,500 per month, is 25% higher than it was last year (and 275% higher than in 2010) and the volume of reports of contact abuse to police also continues to rise. These reports are often unable to be investigated due to the lack of data held by CSPs which would enable identification of individuals who have posted and shared IIOC. The live-streaming of abuse from developing to the developed world is judged to be an emerging threat as access to well-developed internet infrastructure (4G and broadband) increases.

Example: On September 11th 2015, seven men were convicted of child sexual abuse offences and handed sentences totalling 107 years as part of Operation VOICER. His Honour Judge Lambert said during sentencing that this case was 'evil beyond rational understanding'.

This investigation related to an organised crime group (OCG) which coordinated grooming and contact sexual abuse of extremely young infants, in addition to making and distributing Indecent Images of Children (IIoC). The abuse was live streamed using internet based communication services and the images were distributed using social media as well as the wider Internet.

The NCA gathered vital intelligence from numerous devices seized from 12 core suspects which showed frequent messaging via online communication services. This information enabled the investigation to be widened, further identifying 262 other paedophiles involved internationally, a number of which remain unidentified. Usage of these applications is not shown in traditional communication data records.

Bill Provisions: The provisions in the draft Bill that enable ICRs to be requested would certainly assisted in an operation such as VOICER explained above. In this case, access to retained ICRs would have provided vital intelligence to identify who these people are and in turn identify their communications and further linked suspects to enable enforcement action and safeguarding of victims. It is also anticipated that this might have speeded up the investigation so preventing additional harm inflicted on the victims.

This investigation was reliant on seizing suspect devices revealing the extent of communications between child abusers. Much of this information would have been available proactively through CD if ICRs were retained.

Threat: Firearms

Despite reductions in the criminal use of firearms and discharges, the risk from firearms remains serious. Overall, there were 30 fatalities in 2012/13 resulting from offences involving firearms. Firearms continue to enter the criminal market through a variety of means, including direct importation through post/fast parcels and thefts from legitimate firearms holders or dealers.

Over a three month period (May to July 2015) the NCA Border Policing Command (BPC) received 220 detections of firearm seizures from Border Force. 54 of these seizures were firearms.

Impact of the Internet: Criminals acquire firearms from a range of sources, including online sellers (e.g. via the anonymous criminal marketplaces on the darkweb), at militaria fairs and through criminal contacts. Social media and TOR forums are often used as platforms for related discussions and this is of growing concern.

Project EAGLEHEAD is a joint investigation between the NCA and USA's Homeland Security Investigations (HIS) targeting US based sellers that supply UK customers. EAGLEHEAD has led to:

- The recovery of more than 58 firearms by 26 police forces
- The arrest of 21 people and charge of 19 people with firearms offences

Whilst projects such as EAGLEHEAD have been successful at having a positive impact on some US based sellers who are now refusing to sell to UK buyers the investigation is dependent on international cooperation where there is no legal basis for sellers to comply with UK requests and patchy retention of IP data that enables identification of both buyers and sellers.

At present when illegal firearms are found to be posted on legal sites the NCA issues an alert to the website requesting removal of the posting. Little else can be done to trace the individual who has posted these adverts if false account details are provided.

Example: An ongoing investigation into a firearms supplier on the dark web which identified a number of UK based customers is an example of how both the dark web (TOR) and open source websites are used as a source of illegal firearms such as assault rifles, submachine guns, ammunition and associated component parts.

Bill Impact: The draft Bill will enable ICRs to be requested for 'illegal sites' (definition to be clarified) however the restriction placed on wider investigative leads means that Law Enforcement will not be able to request ICRs for legal sites that may sell firearms from other jurisdictions or online marketplaces where Law Enforcement is reliant on 'tip-offs' from the general public or the website itself once an illegal sale is posted. This will leave a big gap in the intelligence picture for law enforcement and negatively impact the ability to trace the source of firearms supply and the networks that are purchasing them.

Threat: Human Trafficking

Human trafficking for sexual exploitation is estimated to cost the UK £890 million each year in addition to the misery inflicted on its victims.

Human trafficking and wider aspects of modern slavery remain a high-priority threat to the UK. Referrals of Potential Victims of Trafficking (PVoT) to the National Referral Mechanism have increased year on year for the past 3 years. The HO estimates that there may have been as many as 10,000 to 13,000 PVoTs in the UK in 2013. Labour exploitation was the most common trafficking type in the UK in 2014, it is likely to remain an increasing risk in 2015.

Impact of the Internet: The internet and mobile technology is now an integral part of the advertisement and 24 hour supply of men and women for all aspects of sexual services. Internet platforms are used for sex workers to advertise their availability and are also used by those who deliberately traffic men and women in and out of the UK for sexual exploitation.

In some instances the individuals who operate these websites take great steps to conceal their identity through obfuscation of the domain's registration details (unique address), similar to the use of off shore shell companies with nominal directors appointed. This is just as likely to be as a means to avoid the tax authorities and pressure from law enforcement than for any other purposes. Other sites are able and do provide intelligence to assist with Law Enforcement investigations.

Whilst overt use of the internet and mobile technology plays an integral role in many aspects of the sex industry (and the exploitation of victims), it is unassessed if the dark web is used in any coordinated way by human traffickers.

Example: An investigation into an Organised Crime Group suspected of involvement in controlling prostitution, human trafficking and money laundering in Northern Ireland with links to Europe highlights the use of the internet to facilitate a traditional crime.

The OCG used an online escort site to advertise the services of victims of trafficking hidden amongst a surplus of other consenting sex workers in order to generate criminal funds. The use of the internet in this case provided multiple evidence and intelligence gathering opportunities in relation to communications data.

Communications Data obtained in relation to these adverts included both traditional call data (telephone numbers) and IP data enabling the identification and location of the victims and organised crime group members. CD was used in conjunction with analysis of account information and photographs which were examined for metadata, common backgrounds, clothing and locations allowed PSNI to identify adverts on other websites around Europe.

Bill Provisions: In this example the investigation would have benefited from access to ICRs for the purposes of identifying additional communication sites that the suspects had visited as this would have provided leads on other sites the sexual exploitation of victims of trafficking were being advertised and identification of the wider criminal network.

The restrictions in the IP Bill to request ICRs for wider investigative services would hamper the investigation since data on banking services used to launder proceeds of crime and travel bookings would have provided key leads of enquiry.

Threat: Missing Persons

The police deal with a missing person's incident every two minutes. Last year 10% of missing incidents (of 211,521 records in 43 forces) were classified as high risk: 60 high risk missing incidents each day of which around 40 will be children. High risk cases require the immediate deployment of police resources. The police investment in high risk cases is a serious resource and financial commitment. 70% of search advisor time is spent on missing incidents. A conservative estimate of the average cost of investigations in high risk cases is between £6,500 and £8,500 (more than £150m each year for all high risk cases). Operational Response: Each of the high risk case investigations will include an assessment of both communications and financial data in the search for and safeguarding of the missing person.

Example: In a missing/abduction case involving a teenager in the north of England, a girl had arranged to meet an older man. The man had been in communication with the girl using numerous online methods with initial contact being made via PlayStation online forums with further conversations enabled via VoIP (Voice-over IP) within an online gaming capacity. It was information from the girl's data which identified the man's device and then identified the location and the hotel.

Bill Provisions: This case could have progressed more quickly with access to Internet Connection Records, especially as the police did not have access to the girl's phone. The communications between the man and his intended victims had been through chat rooms and internet messaging services and not voice or text calls. The case relied on evidence from Communications Data obtained from the seized 'phones and computers, which could have been obtained proactively through ICRs.

In the case above, the Bill provisions would enable investigators to identify the online chat services that the missing child had accessed prior to her disappearance enabling follow up enquiries to be made to the providers of these services and ideally leading to identification of her abductor. However, the restriction on requesting ICRs for wider investigative leads means that Law Enforcement would not be able to request the supporting information on the services accessed by the victim or suspects device that could identify that they had looked at the hotel website and therefore provide investigative leads on where the victim could be located.

Threat: Tax Crime

The cost to the UK from organised criminal attacks on the UK's tax systems is currently estimated at over £5 billion per annum.

Impact of the Internet: Threats and risks to online tax systems are fuelled by anonymity and agility both of which the internet provides. Alongside 'traditional' smuggling and VAT fraud

offences HMRC is seeing a growth in the number – and sophistication - of online attacks. Broadly these fall into two categories:

- The use of stolen identities to submit fictitious returns to generate repayments
- The use of login credentials stolen from customers to acces their accounts and divert repayments or steal confidential data.

In the first case, for example, stolen company payroll data can provide information required to register an unknowing victim for new tax accounts. At the point of registration with HMRC the victim's bank account details will be used but this is likely to be changed following confirmation of a successful login. The only realistic way of investigating this offence is by following communications data identifiers such as the IP address which will be produced at the point of online interaction between the criminal and HMRC. If CSPs do not keep IP address details then the trail will run cold.

In the second case identifying the criminal is the challenge. Access to the hijacked account causes the criminal's IP address to be logged. But more sophisticated criminals will take steps to thwart investigation by traversing through numerous IP addresses across different networks and physical locations.

Example:

HMRC conducted an investigation into an OCG utilising the Department's on-line platforms to register multiple Value Added Tax (VAT) and Income Tax Self Assessment (ITSA) applications using hi-jacked or bogus identities. The OCG masked their identities and locations by utilising internet cafes, WIFI hotspot areas and broadband from the addresses of friends and relatives, to access HMRC's on-line facilities. Once a registration was successful the OCG made small repayment claims which were then gradually increased if the initial repayment was achieved.

Bill Provisions: This operation highlights some of the difficulties HMRC have been experiencing with IP address resolution as in this case HMRC were unable to obtain the IP login histories of several key targets as a consequence the HMRC was unable to identify links in the criminal conspiracy and was not able to use CD to evidence association between conspirators during the subsequent court case.

The provisions in the IP Bill which enable ICRs to be used for IP address resolution would improve HMRC's ability to identify and track individuals who are defrauding the revenue of the UK.

ACPO Data Communications Group

Single Point of Contact Data Survey

Between 4th June – 17th June 2012

SPoC Data Survey Results – 2012

Introduction and Background

This survey looks at the acquisition of communications data and provides the reader with an insight into the usage of such data across UK law enforcement. The survey results provide a very short snapshot of how communications data is used across law enforcement agencies. This data only relates to the acquisition of communications data under Chapter1 Part2 Regulation of Investigatory Powers Act 2000.
This survey was undertaken by 63 UK law enforcement agencies.

The survey took place between the 4th June and 17th June 2012 and requested details to be recorded that covered the following categories:

- Crime type under which the communications data was being requested
- Type of communications data being sought
- Age of communications data
- Grading of data requests
- Data subject identification
- Request identifier types

This survey was undertaken at the point when an application is submitted by the applicant to a SPoC. A SPoC is the Single Point of Contact who is an accredited individual responsible for acquiring the data from communication service provider.
This report will only provide the reader with percentages in relation to the acquisition of communications data. No numbers will be provided due to the interests of national security. ACPO Data Communication Group also provided a commitment to all those who took part in the survey to the fact that the actual numbers relating to the survey will not be published.

Full list of offences listed in descending order

Offences	Percentage
Drug Trafficking	17.7%
Drugs Misc	6.9%
Homicide (Any)	6.7%
Burglary (Res & Non Res)	6.5%
Fraud	6.5%
Missing / vulnerable	5.7%
Firearms	5.2%
Other	4.3%
Harassment & Stalking	3.4%
Malicious Comms	3.2%
Theft	3.0%
Serious Assault	2.9%
Child Abuse	2.9%
Other sexual	2.7%
Armed Robbery	2.7%
Rape	2.4%
Street Robbery	1.6%
Robbery	1.4%
Attempt Murder	1.1%
HMRC Offences	1.1%
Kidnap	1.1%
Terrorism	1.1%
Theft of/from MV	0.8%
Money Laundering	0.7%
Bribery &Corruption	0.7%
Blackmail	0.5%
People Trafficking	0.5%

Offences	Percentage
999	0.5%
E-Crime	0.5%
Immigration	0.4%
Criminal Damage	0.4%
Bail & Courts	0.4%
Conspiracy	0.4%
Agg Burglary	0.4%
Arson	0.3%
Forgery Counterfeit	0.3%
Minor Assault	0.3%
Sexual offences	0.3%
Racial Hatred	0.3%
Threats to kill	0.3%
Gang related	0.3%
Public Order	0.3%
Sexual Other	0.2%
Bomb Hoax	0.1%
Obscene Pubs	0.1%
Sex Industry	0.1%
False Impt	0.1%
Vehicle crime	0.1%
Death by	0.1%
Domestic abuse	0.1%
Explosives	0.1%
Witness intimidation	0.1%

Chart 1:

Chart 1 shows percentages in relation to the crime type that a communications data request was made during the survey period.
The following charts provide further information in relation to specific areas Crime Types, Time Periods (Age of Data) RIPA Request Types, Data Subjects and National Request Prioritisation Grades:

Crime Type

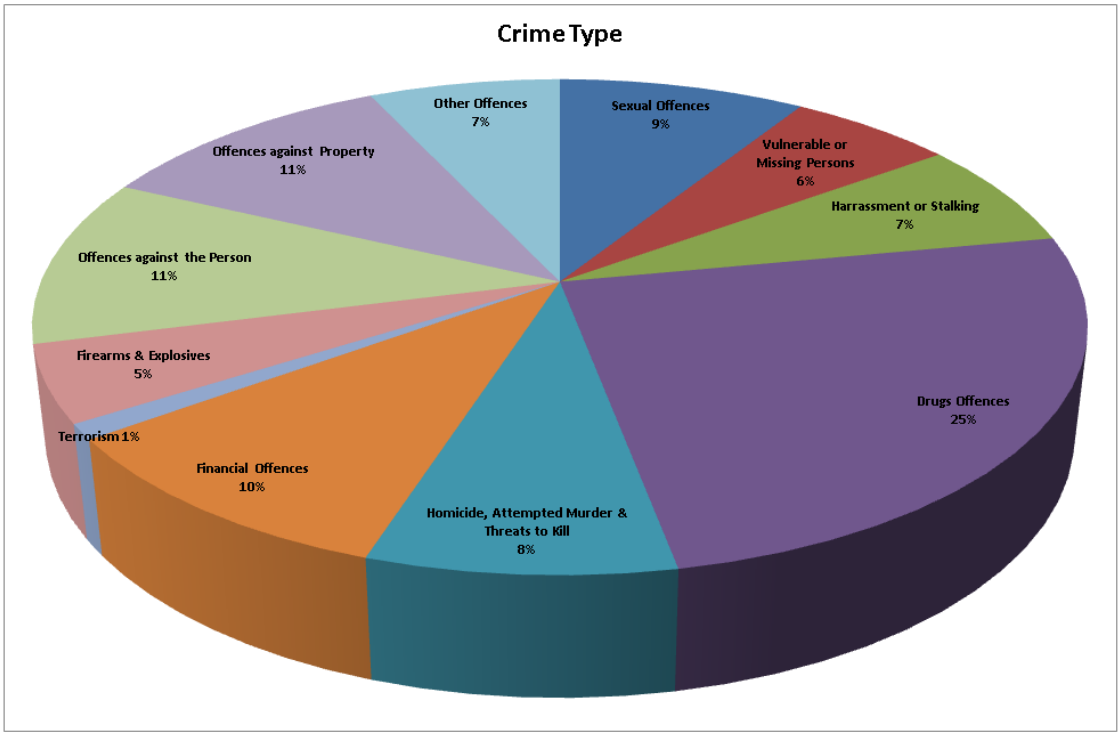


Chart 2: Breakdown of Enquiries by Crime Type

The above chart shows the relative proportions of different crime types for which communications data was requested.

- 25% of communications data requests related to drugs investigations.
- 9% of communications data requests related to sexual offences investigations.
- 6% of communications data requests related to missing/vulnerable persons investigations.
- 8% of communications data requests related to homicide, attempt murder and threats to kill investigations.
- 11% of communications data requests related to property offences, burglary and theft investigations.
- 7% of communications data requests related to harassment and stalking investigations.
- 5% of communications data requests related to firearms and explosives investigations.
- 10% of communications data requests related to financial offences, fraud and money laundering investigations.
- 11% of communications data requests related to offences against the person, robbery, assault, kidnap investigations.
- 7% of other communications data requests related to gangs, arson, bomb hoax and immigration investigations.
- 1% of communication data requests related to terrorism investigations.

Time Periods

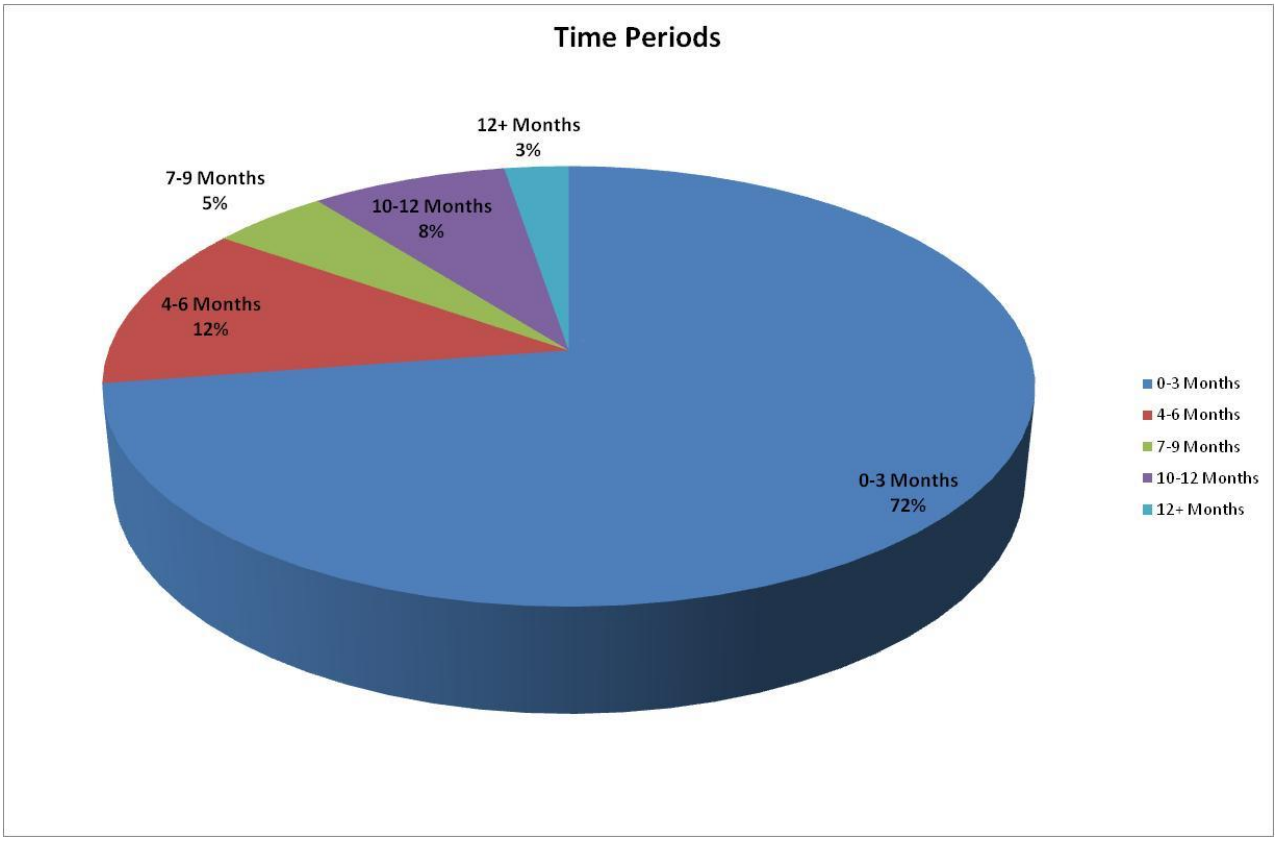


Chart 3: Breakdown of all Enquiries by Time Period

The above chart shows how long communication service providers have held the relevant data that was requested during the survey.
84% of communications data requested was up to 6 months old.
13% of communications data requested was 7 – 12 months old. What should be recognised is that 10-12 months data accounts for 8% this is higher than the 7-9 months data request as investigators realise that they risk losing this data as under the EUDRD, CSPs are not obliged to retain data beyond 12 months.
3% of communications data was more than 12 months old. Although this data does not need to be retained under the EUDRD, this data is retained by some communication service providers for their own business purposes.

RIPA Request Types

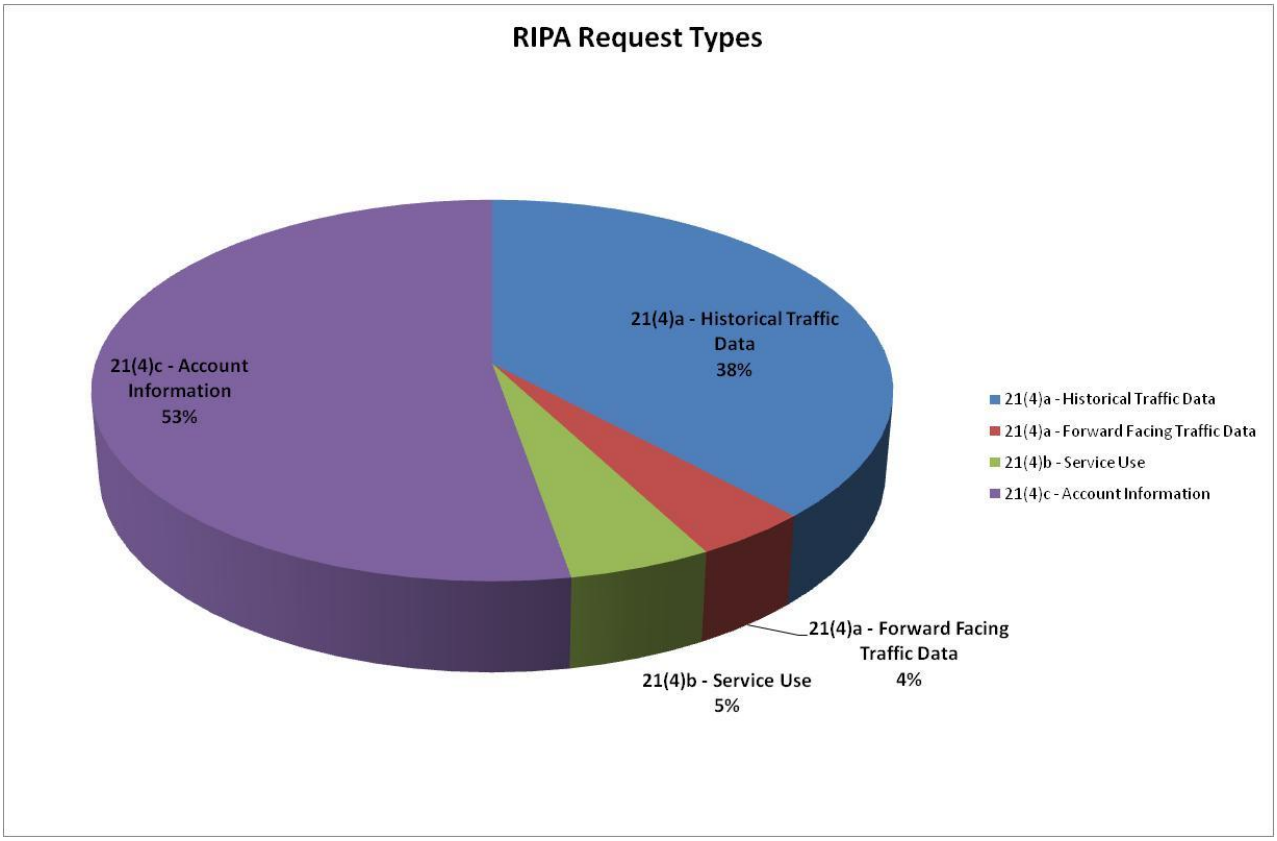


Chart 4: Breakdown of all enquiries by Request Type

Section 24 (1) of RIPA, in this Chapter "communications data" means any of the following:

(a)any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted;

(Historic data requests relate to a date period in the past, whilst Forward Facing data requests relate to dates in the future)

(b) Any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person—

(i) of any postal service or telecommunications service; or

(ii) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system;

(c)any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service.

Data Subjects

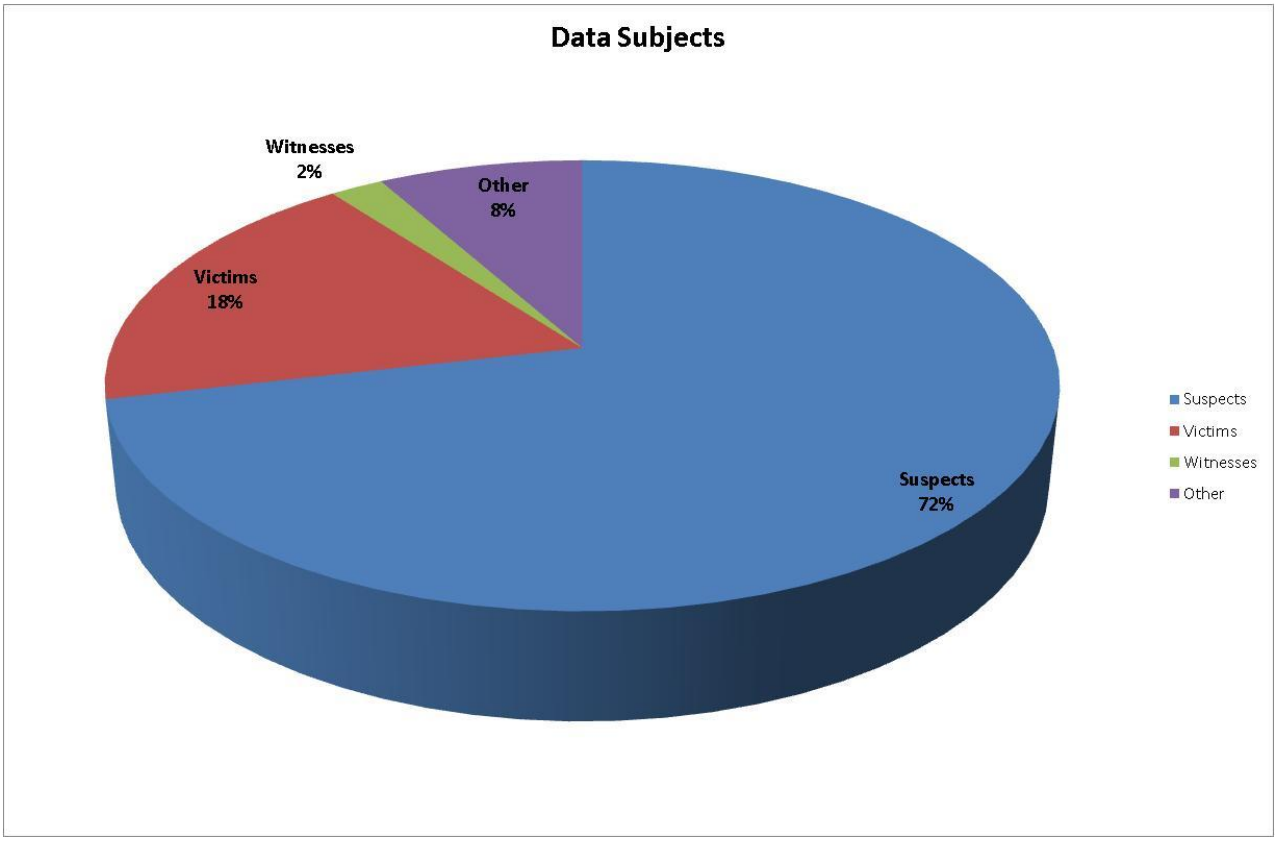


Chart 5: Breakdown of all enquiries by Data Subject types

The above chart identifies the person who the communications data request related to.

72% of the communications data requests related to suspect enquiries; this would clearly be in relation to the prevention and detection of crime. (A suspect is a person who has been arrested charged or believe to be responsible for a criminal offence at a particular time)

18% of the communications data requests related to victims of crime, this could be because their electronic device had been stolen or that communication data was used during the commission of a crime.

2% of the communications data requests related to witnesses, this could be identifying the actual time of a call, identification of a witness through possession of their telephone number.

8% of the communications data requests related to other which could relate to missing persons and vulnerable individuals, persons of interest during a homicide investigation or persons whose status at the time of the submission were unknown.

Whilst this report captures the number of data subjects listed within each application, it is important to remember that multiple applications are often submitted for a single investigation. In this survey 44 investigations accounted for 10 or more RIPA requests. There was one investigation in which over 40 RIPA requests were made.

Grades

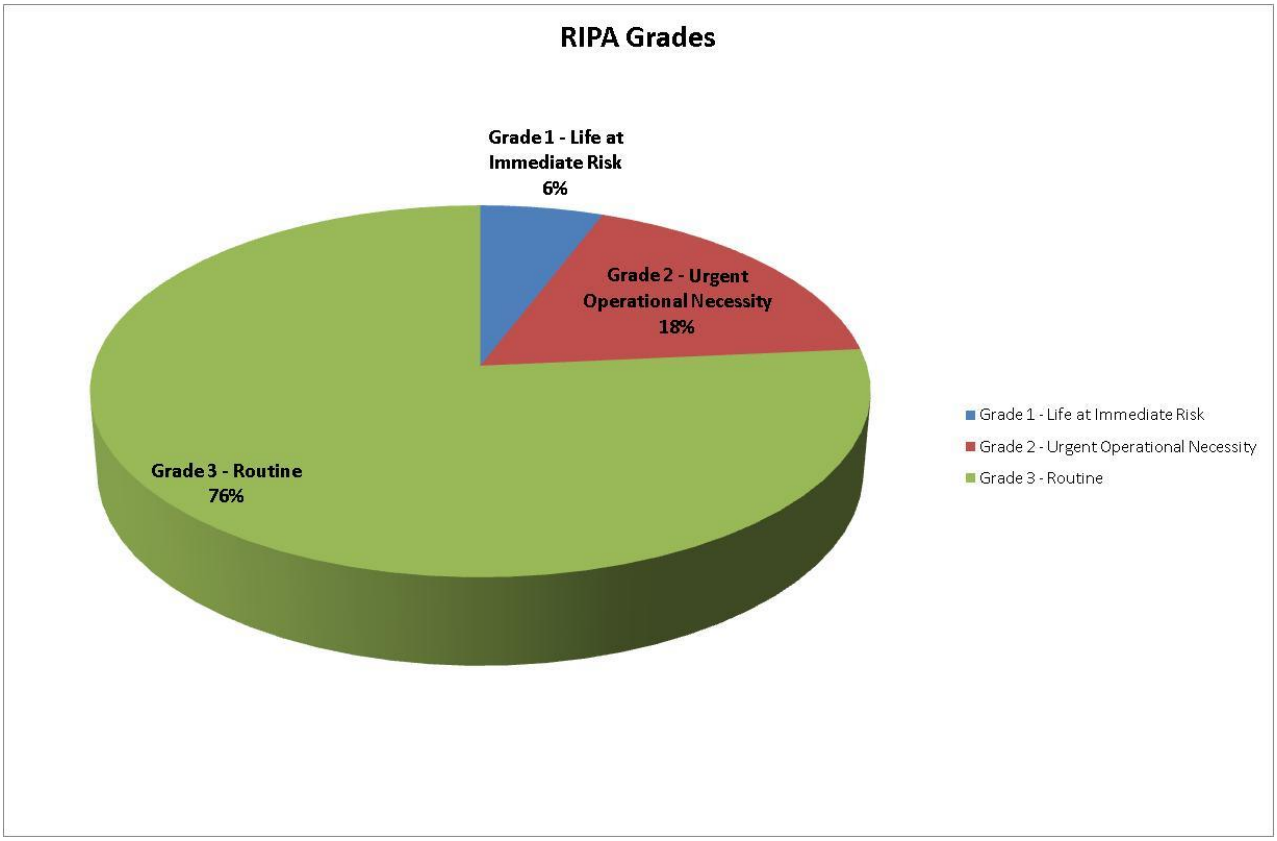


Chart 6: Breakdown of all enquiries by RIPA Grade

The above chart sets out the grade of the communications data request made by law enforcement to the communication service provider.

The Data Communications Group (DCG) which comprises representatives of CSPs, UK law enforcement and other public authorities to manage the strategic relationship between public authorities and the communications industry has adopted a grading scheme to indicate the appropriate timeliness of the response to requirements for disclosure of communications data. There are three grades:

- Grade 1 – an immediate threat to life;
- Grade 2 – an exceptionally urgent operational requirement for the prevention or detection of serious crime or a credible and immediate threat to national security;
- Grade 3 – other enquiries that are less time critical but, where appropriate, will include specific or time critical issues such as bail dates, court dates, or where persons are in custody or where a specific line of investigation into a serious crime and early disclosure by the CSP will directly assist in the prevention or detection of that crime

The emphasis within Grade 1 and 2 is the urgent provision of the communications data will have an immediate and positive impact on the investigation or operation

Significant Findings

What was evident from the survey is the fact that law enforcement is not able to define serious crime. Most definitions that are used are very subjective and what may be classed as serious to one victim may not be serious to another. (This is discussed further at Annex E) The same can be said in relation to other less serious crimes, it is for this reason that we have not included percentages around these areas.

Crime Types

- 25% Drugs Investigations
- 7% Homicide Investigations
- 6% Missing Person and Vulnerable Person Investigations
- 21% Theft Act and Offences Against the Person Investigations

Data requested from communication service providers

- 95% Related to account information or traffic data
- 72% Requests were suspect related
- 20% Requests were victim or witness related
- 24% Requests were due to life at risk or urgent operational necessity

Older data is clearly used less, but data older than 6 months still accounts for a significant number of requests.

- 37% Of data requests relating to sexual offences was older than 6 months
- 27% Of data requests relating to Terrorism was older than 6 months
- 11% Of data requests relating to Drugs was older than 6 months
- 5% Of data requests relating to Homicide/Attempt Murder was older than 6 months
- 9% Of data requests relating to Firearms and Explosives was older than 6 months

Although this survey is only a snap shot over a two week period, this data does provide us with an insight into how, why and for what purpose communication data is used. Unfortunately some of the respondents may have misunderstood the required completion system and submitted data that needed normalisation before being used within this survey (The logic behind this normalisation is available if required).
It is clear that communications data is paramount in enabling law enforcement agencies to protect the vulnerable and saves lives.
Whatever steps criminals take to prevent their apprehension, they inevitably need to communicate with each other, use communication to commit the offence or have communication equipment with them when committing an offence. The increase in communication over the past decade and the increase predicted for the future make it even more important for law enforcement to be able to use the least intrusive investigative technique to prevent and detect crime today and in the future.
The acquisition of communications data is one of the least intrusive investigative techniques undertaken by law enforcement and is a process that is strictly managed and authorised by senior police officers in accordance with RIPA Chapter 1 Part 2.
The process ensures that the designated person complies with the requirements as set out in Chapter 1 Part 2 RIPA giving due consideration to peoples Human Rights, the necessity of the request, it must be for the protection of vulnerable persons or for the purpose of preventing or detecting crime, the authorising officer must be satisfied that it is necessary to use communications data in the investigation.
The proportionality, consideration will be given to balancing the seriousness of the crime being investigated and the interference with the privacy of the individual concerned.
The internal processes implemented and the national governance and inspection regime by IOCCO ensures that this investigative technique is only used in the protection of vulnerable persons and the prevention and detection of crime.

The need for law enforcement to maintain and improve on this capability is fundamental in our ability to keep pace with new technology, protect the vulnerable and continue to prevent and detect crime.

21 December 2015

Law Society of England and Wales—written evidence (IPB0105)

The Law Society of England and Wales is the independent professional body that works to support and represent over 163,000 members, promoting the highest professional standards and the rule of law

1. Legal professional privilege (LPP) is the highest right known to the law. It is over 500 years old and is an essential element of the administration of the justice system in the United Kingdom. Accordingly, LPP is recognised as a fundamental common law right, a human right protected by both Article 6 of the European Convention on Human Rights (ECHR) (Fair Trials) and Article 8 (Privacy). It is also protected under the law of the European Union.

2. LPP is jealously guarded not only by the legal profession but also by the courts, since it is the common law which has shaped the evolution of this right into its present status. That status, and the supremacy of LPP as a right to communicate in absolute secrecy, is fully recognised by Parliament which has ensured that privilege protection provisions are included - with one exception - in every statute and statutory instrument that confer investigatory and evidence gathering powers. The very real consequence of this is that hitherto no state agency or public authority has ever been entitled under English law to compel a citizen or their lawyer to reveal the contents of their communications. In short, English law confers an absolute protection upon LPP which can never be overridden even if this means that, for example, the police (and other law enforcement agencies) and indeed the Courts are potentially deprived of relevant (even crucial) evidence or information.

3. The draft Investigatory Powers Bill (draft Bill), along with the existing Regulation of Investigatory Powers Act 2000 (RIPA), is unique in failing to recognise the supremacy of LPP and to accord it appropriate protection. In reluctantly accepting by a majority that it was Parliament's intention in RIPA to permit the use of covert surveillance techniques to be used in certain circumstances to listen in to privileged conversations between clients and lawyers, thereby infringing the clients' LPP, the House of Lords in McE (2009) nevertheless warned of the very real 'chilling effect' that such surveillance activities can have on the effectiveness and openness which are vital to communications between lawyer and client. They proceeded quite clearly on the basis that such interference should therefore happen but rarely.

4. What we know now from cases like *Belhadj*[710], which have come to light in the last year, is that whereas we thought that interference with privilege under RIPA and related legislation including the Telecommunications Act 1984 and the Intelligence Services Act 1994 was exceptional, the probability is that it is happening on a more routine basis. Such routine interference undoubtedly triggers the chilling effect that concerned the House of Lords. This not only has the potential to undermine Articles 6 and 8 of the ECHR but, more immediately, it undermines the administration of justice as clients censor the information they provide to their lawyers. There is a real risk that incomplete facts are put before the court, or clients represent themselves and fail to run appropriate defences.

[710] [2015] UKIPTrib 13_132_H

5. It is also increasingly clear that communications data can be subject to LPP - a fact that is recognised by neither RIPA nor the draft Bill. In contrast, the European Court of Justice (CJEU) was alert to this in *Digital Rights Ireland*.[711] In part this may have been due to the increasing sophistication of communications data which may disclose not only the existence of a lawyer-client relationship but also the substance of the advice sought and given. Additionally, the failure to recognise that communications data can be subject to LPP overlooks that on occasions client identity and client whereabouts have been recognised as matters within the scope of the client's privilege.

6. There is very little evidence that LPP is abused by lawyers or their clients. Where it is, no privilege applies. This is because of the operation of the well-known 'crime-fraud' or 'iniquity exception' that allows the contents of such communications to be revealed in such circumstances. Given that there can never be a legitimate interest in listening into proper communications between clients and lawyers, even applying the exception has to be undertaken with considerable care. The exception can provide an accepted basis for intruding on client-lawyer communications but this has to be allowed only on the clearest of bases where there is compelling evidence that the privilege is being abused. It cannot be done on the basis of a mere suspicion.

7. The Law Society recommends that the draft Bill should be amended to include:

- Express recognition of the importance of LPP on the face of the Bill, allied with appropriate protection that makes it clear that privileged communications are simply off limits. This protection should cover all forms of investigatory powers, including the acquisition of communications data

- Provisions that ensure that the deliberate targeting of legally privileged communications, material, information and data are unlawful.

Accordingly, we endorse the initial draft New Clauses proposed by the Bar Council for the protection of LPP.

8. We believe that seeking to protect LPP merely via codes of practice is inadequate, as well-known recent cases have demonstrated. Codes of practice are, of course, helpful and have their place if clearly drafted, but privilege is such an extraordinary right that it has to be protected in the primary legislation - as has been the practice of Parliament in hundreds of other instances. Judicial oversight of the application process as currently proposed is very welcome, and would be an adequate protection, so long as the ambiguity created by reference to the 'judicial review' standard is removed from ss.19(2) and 90(2) of the draft Bill *and* there was an express recognition in the statute that that privileged material is excluded. The Judicial Commissioner reviewing the Home Secretary's decision would then simply have to decide if the iniquity exception applied.

Further Information

[711] Case C-293/12

9. The relationship between LPP and the State's current investigatory powers regime is explored in depth in a position paper produced by the Bar Council and the Law Society and supported by the Bar of Northern Ireland and the Faculty of Advocates.[712] The Joint Committee has seen this paper in which we argue that LPP is a "fundamental condition on which the administration of justice as a whole rests"[713] whose importance cannot be overstated.

We argue that LPP is a cornerstone of a society governed by the rule of law, ensuring that persons are able to consult a legal adviser in absolute confidence, and safe in the knowledge that there is no risk that information exchanged between lawyer and client will become known to third parties without the client's clear authority. We also argue that the 'iniquity exception' controls the rare occasions on which privilege is abused by removing from the scope of privilege communications made in furtherance of a criminal purpose.

10. Like RIPA, the draft Bill fails to protect LPP. It is silent about protection for LPP in relation to interception of communications and equipment interference and it incorrectly holds that communications data cannot attract LPP.

The chilling effect

11. We are concerned about the 'chilling effect' of surveillance. Although s.42 of the draft Bill (like s.17 RIPA) excludes intercepted material from legal proceedings and therefore warranted interception can only be used for intelligence purposes, the possibility of monitoring in itself engenders a deep uncertainty that has the potential to undermine individual rights and the administration of justice. Both the telescreens in Orwell's 1984 and Jeremy Bentham's design for a Panopticon were based on a similar uncertainty as to when surveillance was taking place.

In *McE* (1999),[714] Lord Phillips suggested that it would be desirable, if not essential, "to reassure those in custody that, save in exceptional circumstances, their consultations with their lawyers will take place in private. The chilling factor that LPP is intended to prevent will not then occur" (para 51). In the same case Lord Neuberger pointed out that "it is self-evident that knowing that a consultation or the communication may be the subject of surveillance could have a chilling effect on the openness which should govern communications between lawyer and client" (para 111).

12. Since the decision of the Investigatory Powers Tribunal in the *Belhadj* case, in which it determined that there had been an infringement of Article 8 in respect of legally privileged information held by GCHQ, it has become clear that surveillance of legally privileged communications are not as rare as had been assumed. The Agencies have had longstanding guidance on the treatment of legally privileged material and the Interception of Communications Commissioner appears to make regular recommendations involving the treatment of LPP.[715]

---

[712] Investigatory Powers and Legal Professional Privilege (October 2015) https://www.lawsociety.org.uk/news/documents/position-paper-investigatory-powers-legal-professional-privilege-october-2015/

[713] *R v Derby Magistrates' Court, Ex p B* [1996] AC 487, *per* Lord Taylor LCJ at 507

[714] *McE v Prison Service of Northern Ireland, C v Chief Constable of the Police Service of Northern Ireland* [2009] UKHL 15

[715] Report of the Interception of Communications Commissioner, March 2015.

None of this is enough: the chilling effect that this undoubtedly creates is only compounded by the powers contained in the draft Bill that would allow potentially far more intrusive 'equipment interference'.

Communications data

13. Communications data are often presented as being relatively less intrusive than access to the content of a communication. In relation to obtaining or holding communications data, Schedule 6 of the draft Bill provides that the Secretary of State must issue a code of practice which includes "provision about particular considerations applicable to any data which relates to a member of a profession which routinely holds legally privileged information". This is both inadequate and, in any event, far from clear.

14. In the *Guide to Powers and Safeguards* published alongside the draft Bill, the section dealing with *Protections for Communications Involving Sensitive Professions* argues that "accessing the communications data of an individual does not disclose what that person wrote or said, rather when they communicated, where, how and with whom. Communications data does therefore not attract, for example, legal professional privilege in the same way as the content of a communication between lawyer and client." (para 52).

15. The Law Society maintains its strong disagreement with this view that was set out in our joint position paper with the Bar Council, where we argued that "Access to CD now enables the authorities to piece together a very complete picture of what the contents of a communication might look like. As technology has advanced, there is a diminishing distinction between CD and its content in terms of what we can learn about the target. CD may disclose not only the existence of the lawyer-client relationship but also the substance of the advice sought and given (for example the identity of an expert witness who has been cc'd into an email). Accordingly, the argument that CD is not covered by LPP is no longer tenable." (para.14).

16. It follows that access to legally privileged communications data should be protected by provisions on the face of the Bill and by adequate judicial oversight arrangements.

17. The question of retention of communications data was addressed in the *Digital Rights Ireland* case by the CJEU. The Court laid down what some consider to have been mandatory criteria to be met by all national legislation providing for access to and use of retained communications data. It is noteworthy that in its judgment the CJEU referred to the absence of any exceptions in the EU Data Retention Directive for persons "whose communications are subject, according to rules of national law, to the obligation of professional secrecy." This pre-eminently includes communications between lawyers and their clients.
That case was considered by the Court of Appeal recently in the Secretary of State for the Home Department v Brice, Lewis, Davis and Watson, in which the Law Society, Open Rights Group and Privacy International have intervened. The Court of Appeal observed that the central issue in the case was the effect of the judgment in Digital Rights Ireland. It has referred the case to the CJEU because 'the true effect of the judgment in Digital Rights Ireland will remain central to the validity of all future legislation enacted by the member

states in this field.' It has asked the CJEU to consider whether the criteria in Digital Rights Ireland are mandatory. Even if the CJEU were to decide that Digital Rights Ireland did not lay down mandatory criteria for the protection legal privilege in legislation dealing with access to and use of retained communications data, there would be nothing to prevent Parliament from doing and it should do so given the importance of legal privilege as a corner stone of the rule of law.

Judicial oversight

18. Sections 19 and 90 provide, respectively, for approval of interception and equipment interference warrants by Judicial Commissioners. They must approve the original issue of the warrant on the basis of whether it was *necessary* on relevant grounds and whether it was *proportionate*. However, in doing so they must "apply the same principles as would be applied by a court on an application for judicial review" (ss. 19(2) and 90(2)).

19. The House of Commons Library briefing paper[716]notes that this apparent qualification to the oversight provided by the Judicial Commissioners has been described by Liberty as involving "a highly limited review which will in practice be a rubber stamping exercise", whilst Lord Pannick QC has argued that judges applying a judicial review test must still consider the merits.

20. It appears to be the Government's intention that oversight by Judicial Commissioners should not be a 'rubber stamping' exercise and the Law Society would argue that this should be made plain, and all ambiguity avoided, by removing sections 19(2) and 90(2).

21 December 2015

[716] Draft Investigatory Powers Bill, Briefing Paper 7371, 19 November 2015

The Law Society of Scotland—written evidence (IPB0128)

December 2015

Introduction

The Law Society of Scotland is the professional body for over 11,000 Scottish solicitors. With our overarching objective of leading legal excellence, we strive to excel and to be a world-class professional body, understanding and serving the needs of our members and the public. We set and uphold standards to ensure the provision of excellent legal services and ensure the public can have confidence in Scotland's solicitor profession.

We have a statutory duty to work in the public interest, a duty which we are strongly committed to achieving through our work to promote a strong, varied and effective solicitor profession working in the interests of the public and protecting and promoting the rule of law. We seek to influence the creation of a fairer and more just society through our active engagement with the Scottish and United Kingdom governments, parliaments, wider stakeholders and our membership.

We are pleased to consider and respond to the UK Parliament's Joint Committee (the Committee) call for written evidence on the Draft Investigatory Powers Bill. This response has been prepared on behalf of the Law Society of Scotland by members of our Privacy Law Committee.

General Comments

The provisions of the draft Bill have serious implications for the rights of individuals. In a democratic society, it is essential for legislation, such as this, to be sufficiently debated and scrutinised. Such scrutiny is essential to maintain public trust and confidence in the legislative process and to ensure that the Bill is competent in meeting the policy and intent objectives.

<u>Professional legal privilege</u>

On the 14 December we provided oral evidence to the Joint Committee, alongside the Law Society of England and Wales, expressing our shared and serious concerns in relation to professional legal privilege and the provisions of the Bill. Legal professional privilege (LPP) is key to the rule of law and is essential to the administration of justice as it permits information to be exchanged between a lawyer and client without fear of it becoming known to a third party without the clear permission of the client. Many UK statutes give express protection of LPP and it is vigorously protected by the courts. The 'iniquity exception' alleviates concerns that LPP may be used to protect communications between a lawyer and client which are being used for a criminal purpose. Such purpose removes the protection from the communications, allowing them to be targeted using existing powers and not breaching LPP.

We feel that it is essential that LPP is expressly protected in the proposed legislation. The proposal to protect it through a Code of Practice (CoP) is not satisfactory and is also very unusual. All other legislation, which relates to investigatory powers expressly provides for LLP within the provisions of the relevant Act. We suggest that no clear evidence or

reasoning has been provided to demonstrate or explain the absence of the protection of LLP within the Bill and why this should be in a CoP. We would welcome clarification from the UK Government of the reason for this. A CoP does not have the force of law, giving the possibility of abuse. Deliberate targeting of communications covered by LPP needs to be declared unlawful.

In the evolving world of communications it is also important to consider what aspects of communication should be covered by LPP. Clearly content is an essential component. However, communications data can reveal a great deal about the interaction between a lawyer and client. For example communication with a specific expert witness can reveal a great deal about the subject matter of other communications.

Collection of large quantities of data relating to large numbers of people in a fairly indiscriminate fashion will inevitably result in collecting data relating to lawyer-client communications: this requires protection. Such large scale collection of data is in any case likely to be in contravention of EU law subsequent to the decision of the Grand Chamber of the Court of Justice of the European Union (CJEU) in the joined cases brought by Digital Rights Ireland (C-293/12)[717] and Seitlinger and Others (C-594/12)[718] handed down on 8 April 2014

Communications Service Providers retaining data

We are concerned about the requirement for Communications Service Providers (CSPs) to retain communications data. Given the remarkable number of data breaches suffered by commercial organisations in recent months we are not convinced that CSPs will be in a position to store such data securely. Cybercriminals are likely to see such repositories as prime targets, with the data giving the potential for a wide range of crimes including terrorist and hate crimes targeting minority groups, which could fairly easily be identified. We feel it would be appropriate for a state agency to be created with specific responsibility for the secure storage of this data.

Comments relating to specific clauses

We note that clause 2 creates the offence of unlawful interception. By virtue of clause 2 (1) (a) (iii) this will include '*a public postal service'.* However, we further note that private postal services is not included, and does not appear to have been considered. Many businesses, including legal service providers such as solicitors, use private postal services (e.g Legal Post, DX etc) to send sensitive and confidential documents and information. We would suggest that given the possible confidential nature of the communication, private postal services should also be included within the Bill and afforded the protection which clause 2 seeks to achieve.

Clause 6 relates to monetary penalties for certain unlawful interception. We note that clause 6(6) and schedule 1 paragraph 4 (4) (g) a person may request an oral hearing before the Commissioner to make representations. It is not clear from the provisions if such a person may have legal representation and if so if legal aid will be available. We would

[717] http://curia.europa.eu/juris/document/document.jsf?docid=150642&doclang=EN
[718] Ibid

welcome clarification from the UK Government, and would suggest that given the nature of the Bill and from an equality of arms perspective, legal representation should be available as a right.

We note that clause 7 (1)(a)(b) refers to EU instruments and international agreements. We would suggest that this is vague and in the interests of clarity and certainty, any such agreements or instruments should be expressly listed and set out on the face of the Bill. Thereafter, any modifications to such a list must, we believe, be subject to full scrutiny before such time as the modifications are applied.

Clause 12 (c) refers to disclosure of intercepted material to the person to whom the warrant is addressed or any person acting on that persons behalf. What is the link between theses persons, and how is this to be demonstrated and proved? We would also suggest that clause 12 (5) provides for very wide, potentially too wide, powers by authorising 'any conduct by 'any person'. The wording 'any conduct' is, we suggest, ambiguous and may have the effect of conferring unfettered and unintended powers on 'any person'. The powers conferred, we suggest, must be listed fully within the Bill.

Clause 13 relates to the subject matter of the warrants. We note that this may be a single set of premises or a particular person. What will be the position if neither of these can be ascertained with any certainty?

Clause 14 provides power to the Secretary of State to issue warrants. We would suggest that all applications for a warrant should be considered and issued by a member of the Judiciary who is independent of Government. It is important to recognise that such a warrant has Article 8 (right to private and family life) implications and any powers must be balanced with those rights. This same observation also applies to clauses 17, 84, 85 and 86.

Clause(s) 16 and 17 relate to protection for Members of Parliament and powers to Scottish Minister to issue warrants respectively. We note that clause 16 (2) requires the Secretary of State to consult with the Prime Minister where any application relates to 'a member of the Scottish Parliament'. We would suggest that the duty to consult should also include the head of the relevant devolved administration, such as the First Minister for Scotland.

Clause 26 relates to modification of warrants. We note that major modifications can be made by Secretary of State, a member of the Scottish Government or a senior official acting on their behalf. Clause 26 (6) also permits minor modification, in addition to those mentioned, by *'the person to whom the warrant is issued'*. We would, reflecting our earlier comments in relation to considering and granting applications for warrants, suggest that modification, major and minor be only made with judicial agreement. These same comments also relate to clauses 95 and 96.

Clause 27, cancellation of warrants. We would suggest that where a warrant is to be cancelled, then a report should be submitted to the Judicial Commissioner or the authorising person setting out fully the reasons for cancelling. These same comments also relate to clause 98.

In relation to special rules for certain mutual assistance warrants, clause 28. As with our earlier comments to clause 7, we would suggests that in clause 28 (1)(a) any such assistance agreements or instruments should be expressly listed and set out on the face of the Bill. Thereafter, any modifications to such a list must, we believe, be subject to full scrutiny before such time as the modifications are applied.

Clause 35 provides the power to intercept postal communications done in accordance with the Postal Services Act 2000 or 'another enactment'. This is very vague, what is another enactment? We would welcome clarification from the UK Government.

We note that clause 38 authorises 'interception' in the State Hospital (Scotland's high security psychiatric hospital) if it is conduct in pursuance of, and in accordance with, any direction given to the State Hospitals Board for Scotland under section 2(5) of the National Health Service (Scotland) Act 1978. We further note that the provision of clause 38 appears to fail to take into account the current framework for the interception of postal correspondence and telephone calls in psychiatric hospitals within Scotland. The current statutory framework is set out in sections 281-286 of the Mental Health (Care and Treatment) (Scotland) Act 2003, and supplemented by the Mental Health (Specified Persons' Correspondence) (Scotland) Regulations 2005.[719] Section 284 provides for regulations on the use of telephones (including interception), and section 285 gives a direction-making power to Scottish Ministers as to the implementation by hospital managers of those regulations[720].

We are concerned at this apparent oversight and suggest that the provisions of clause 38 should expressly provide that any action which is authorised under the 2003 Act is lawful. We would further suggest that without clear justification, the Bill should not add another route to authorising interception in a psychiatric hospital when there is already a statutory regime covering this. To do so may, we believe, result in confusion.

Clause 171 relates to error reporting. The provisions of the clause refer to 'relevant error' 'serious error' and 'error' throughout. These terms appear to be used interchangeably throughout the clause. Clause 171(11) attempts to provide a definition of 'relevant error'. However, there is no definition provided for 'error' or 'serious error'. In the absence of a definition, these may be defined either widely or narrowly.

Clause 177 provides the Secretary of State with powers to modify, by regulations, the functions of the Investigatory Powers Commissioner, or any other Judicial Commissioner. We also note, that in exercising this power, the Secretary of State may be exercised by modifying any provisions made by or under an enactment. We suggest, and we are concerned, that these powers are exceptionally wide and draconian, effectively amounting to 'Henry VIII powers'. There is no obligation to consult before making such modifications and there is no apparent oversight to ensure there is no excessive dilution of privacy rights.

[719] http://www.legislation.gov.uk/ssi/2005/408/made/data.pdf
[720] See the Mental Health (Use of Telephones) (Scotland) Regulations 2005 (SSI 2005/468) http://www.legislation.gov.uk/ssi/2005/468/made/data.pdf

Also, it would appear there is no reasonable restriction on how the powers may be exercised.

22 December 2015

Liberty—written evidence (IPB0143)

About Liberty

Liberty (The National Council for Civil Liberties) is one of the UK's leading civil liberties and human rights organisations. Liberty works to promote human rights and protect civil liberties through a combination of test case litigation, lobbying, campaigning and research.

Liberty Policy

Liberty provides policy responses to Government consultations on all issues which have implications for human rights and civil liberties. We also submit evidence to Select Committees, Inquiries and other policy fora, and undertake independent, funded research.

Liberty's policy papers are available at
http://www.liberty-human-rights.org.uk/policy/

Executive Summary

Liberty welcomes the publication of a new law to regulate State surveillance in the UK. We support the lawful, targeted and proportionate use of intrusive powers to detect and prevent serious crime. But since the inception of the Regulation of Investigatory Powers Act 2000 (RIPA) we have argued that the authorisation, scope and oversight arrangements for the UK's surveillance regime are in need of urgent and radical overhaul. The Government's Reviewer of Terrorism's investigatory powers review condemned the status quo under RIPA and other enabling legislation as *"undemocratic, unnecessary and – in the long run – intolerable."*[721] This stark and realistic assessment of the need for transparency and reform was in glaring contrast to the Government's repeated claims since 2013 that the current legislative framework contains "robust" safeguards to meet our human rights obligations.

The Snowden revelations of 2013 and subsequent litigation brought by Liberty and others shows how far we have moved from a model whereby those under suspicion are targeted and the innocent are left free from state intrusion. We have in so doing moved far away from the requirements of human rights law. Liberty currently has litigation pending both before the European Court of Human Rights (ECtHR) in Strasbourg & the Court of Justice of the European Union (CJEU) challenging key aspects of the current legislative framework which is replicated and extended in the Draft Bill. While we await further judgment in both cases, the CJEU judgment in *Digital Rights Ireland*[722] in 2014 and the recent judgment of the ECtHR in *Roman Zakharov v Russia*[723] are instructive on the many ways in which the Draft Bill falls woefully short of ECHR standards.

This briefing examines the various powers, mechanisms and purported safeguards in the Draft Bill. We identify a number of the ways in which the claims made about the value and

[721] David Anderson QC, A Question of Trust, paragraph 35.
[722] *Digital Rights Ireland (C-293/12) and Seitlinger and Others* (C-594/12).
[723] Roman Zakharov v. Russia, 4th December 2015,*(Application no. 47143/06)* available at - http://hudoc.echr.coe.int/eng-press#{"itemid":["001-159324"]}

utility of the Bill are not supported by the evidence. We examine and make recommendations on the **process for authorisation of surveillance warrants** and in particular the need for **one-stage judicial authorisation for all warrants** and **reform of the legal tests** for the use of intrusive powers. We **critique the existing framework for communications data retention and acquisition replicated at Parts 3 & 4 of the Draft Bill and challenge the so-called operational case for bulk 'ICR' retention and the Request Filter.** We make recommendations **to improve the system for targeted interception contained in Part 2 and targeted hacking in Part 5 to make both capabilities compliant with our human rights framework and capable of producing legitimate and reliable evidence in criminal trials.**

We examine the Part 6 & 7 proposals to legislate for **new and unusual mass surveillance powers**, including: bulk interception; bulk communications data acquisition; bulk hacking and the acquisition of Bulk Personal Datasets and make the **case against mass surveillance which is simultaneously unnecessary, disproportionate, counter-productive and a stain on our human rights record**. **We suggest reforms to provide overdue statutory protection to the confidential and privileged communications of MPs, Peers, MSPs, AMs, MLAs, MEPs, journalists and lawyers**. We point out the many ways in which the authorities can use targeted means to seek access to suspicious encrypted communications and **advocate for the preservation and promotion of global encryption standards** as an increasingly important social good. We comment on the **absence of a statutory framework for intelligence sharing in the Draft Bill** and examine proposed changes to the oversight regime, arguing for **the conflicting functions of the newly created Investigatory Powers Commission to be vested in two institutionally separate bodies and for the creation of a legislative presumption in favour of post-notification to those subjected to targeted surveillance.**

The authorisation process for surveillance warrants

1. The Draft Bill retains the power for the Secretary of State to issue interception warrants and provides new powers for the Secretary of State to issue hacking and bulk warrants. Bulk and targeted warrants of all types are issued by the Secretary of State, on application from the three intelligence agencies, where she considers it necessary and proportionate on the basis of three broad grounds.[724] The Secretary of State can also issue targeted interception and targeted hacking warrants to a range of law enforcement bodies. Chief constables are granted the power to issue targeted hacking warrants on application from police constables.

2. The process for issuing warrants is similar to the present process for issuing interception warrants subject to a new requirement for a judicial commissioner (JC) to review a warrant before it is issued. The Bill stresses that the decision to issue a warrant is taken *personally* by the relevant Minister or, in urgent cases, by a designated senior civil servant.[725] The Bill states in terms that a "judicial commissioner" is restricted to reviewing a minister's conclusions by *"applying the same principles as would be applied by a court on application for judicial review."*[726] If a JC decides to refuse to approve a

[724] In the interests of national security; for the purpose of preventing or detecting serious crime; and in the economic interests of the UK, so far as those interests relate to national security.
[725] Clauses 22, 88, 110, 124, 139, 158.
[726] For example clause 19. See also 90, 109, 123, 138, 155.

decision to issue a warrant he/she must give reasons and the Minister issuing the warrant can make a fresh application to the Investigatory Powers Commissioner (IPCr).[727] Warrants can last for 6 months and be renewed indefinitely. Surprisingly, the Bill provides for many types of warrant to be retrospectively modified without judicial authorisation. Modifications can relate to the names, premises, organisations etc. to be targeted. Warrants that are no longer considered justified are to be cancelled by Ministers rather than JCs. In urgent cases warrants can be issued without the authorisation of a JC, but the JC must give ex post facto authorisation within 5 days. In these circumstances a JC may, but is not required to, order the destruction of the material obtained. There is no requirement for JCs to notify those subjected to surveillance after the surveillance has ceased.

3. Part 8 of the Draft Bill provides for the creation of the IPCr and the JCs who will be appointed directly by the Prime Minister, for three year renewable terms, following consultation with the Scottish Ministers and the First Minister and Deputy First Minister in NI.[728] The Commissioners functions are twofold: to review surveillance warrants issued by Ministers and to undertake the oversight functions currently carried out by a plethora of different surveillance commissioners. The Secretary of State responsible for providing the judicial commissioners with such staff, accommodation, equipment and other facilities as she considers necessary for carrying their functions. By clause 177, she is able to modify the functions of the JCs by regulations. JCs may be removed from office by the IPCr (on consultation with the PM) on the ground of inability or misbehaviour or a ground specified in the JC's terms and conditions of appointment.[729]

4. Liberty has long called for judicial authorisation for all public authority requests to conduct surveillance. It is the proper constitutional function of the independent judiciary to act as a check on the use of intrusive and coercive powers by State bodies and to oversee the application of the law to individuals. Additionally, judges are professionally best equipped to apply the legal tests of necessity and proportionality to ensure that surveillance is conducted lawfully. English law has long recognised the need for a specific judicial warrant before a person's home can be searched by police when serious crime is suspected, but sadly the process for authorising electronic surveillance has lagged behind. Liberty was therefore delighted when the Government's own Reviewer of Terrorism legislation, David Anderson QC, recommended judicial authorisation for intrusive surveillance, following the most comprehensive review of investigatory powers undertaken in a generation. As the Reviewer observed, making judges responsible for issuing warrants would improve public trust and confidence in the system of surveillance.

5. Liberty believes that the authorisation system laid out in the Bill is wholly inadequate for the UK to fulfil its human rights obligations and to provide a 'world leading oversight

[727] For example clause 19(5).
[728] Clause 167 gives the PM the power to appoint the IPC and JCs from those who have held high judicial office.
[729] Clause 168 (5) provides that Commissioners can be removed from office if convicted of an imprisonable offence, bankruptcy and a range of court orders – insolvency etc. But clause 168(6) further provides that Commissioners may be removed from office by the IPC (on consultation with the PM) on the ground of inability or misbehaviour or a ground specified in the JC's terms and conditions of appointment. Otherwise, Commissioners cannot be removed from office without a resolution approving removal being approved by both Houses of Parliament.

regime'[730]. The JC powers are so circumscribed that the Bill risks creating the illusion of judicial control over surveillance while achieving little change from the status quo. Parliamentarians who would like to see a substantive role for the judiciary in authorising surveillance warrants should support a straightforward one-stage process that gives the task to a JC and removes Ministers' involvement.

Judicial review is not judicial authorisation

6. The Government has sought to portray the authorisation process as a "double lock" implying that both the Minister and the judge have a substantive role in issuing warrants. This is highly misleading. The Bill sets out that the judicial review standard should be applied when JCs consider warrants issued by the Secretary of State. In conducting judicial review of Executive decisions the courts apply a varying standard of review that is highly dependent on the context of the matter before it. At one end of the spectrum is a strict "Wednesbury" standard of review which will only interfere with an Executive decision that is manifestly unreasonable. At the other end of the spectrum is a more intense standard of review that will substantively assess the proportionality of the Executive decision.

7. It has been argued that in the context of the authorisation process in the Draft Bill the more intensive standard of review will be triggered. The point has been made that in a case concerning control orders, *MB,* the Court of Appeal stated that judges applying a judicial review test must consider the merits and decide whether the measure is indeed necessary and proportionate. It is true that the courts have taken a more substantive approach to judicial review in relation to control order and TPIMs cases. But these types of cases, which deal with severe infringements on liberty, do not set a general rule for the standard of judicial review. In fact the intensity of the review to be applied in loss of liberty cases will likely be at the highest end of the spectrum. This is because the liberty of the individual is one of the more tightly protected freedoms in the HRA and at common law; while it is not absolute, it can only be limited in six tightly defined circumstances and for no longer than is necessary.

8. By contrast the Supreme Court held in *Tariq* in 2011 that in civil proceedings not related to any deprivation of liberty, the requirements of *MB* and related cases could be watered down.[731] This case concerned an immigration officer who had his security clearance revoked by the Home Office which resulted in his suspension. He claimed the Home Office had unlawfully discriminated against him on grounds of his religion and ethnicity. Lord Mance, speaking for the majority, said that TPIMs "*impinge directly on personal freedom and liberty in a way to which Mr Tariq cannot be said to be exposed*"[732] and made clear that in cases not concerning the liberty of the individual the standard of review will be different. If the Supreme Court felt unable to apply an intensive standard of review in Tariq, in circumstances where a man had lost his job and feared discrimination on the part of his employer, then a JC is highly unlikely to invoke an intensive standard of review in the context of a privacy intrusion where the practical and

[730] Secretary of State for the Home Office the Right Honourable Theresa May, Oral Statement to Parliament on 4 November 2015.
[731] *Home Office v Tariq,* [2011] UKSC 35.
[732] *Home Office v Tariq,* paragraph 27.

tangible consequences of infringement can be said to be much less immediate and obvious. The standard of review will be further influenced by the extreme deference that will be shown to those warrants that concern national security.[733] JCs may therefore consider themselves unable to refuse a warrant unless it is so manifestly unreasonable that no reasonable Minister could have decided to issue it.

9. A merits review is also made practically impossible by the two-stage model in the Bill. The issuing authority will be the body with the practical ability to probe and test the requesting agency or law enforcement body as to the necessity and proportionality of a warrant. The secondary role given to JCs under the model in the Bill will mean that JCs are restricted to considering ministerial decisions to issue warrants on the papers, in secret, with no opportunity to question the requesting agency, nor to probe as to whether less intrusive methods or capabilities could be deployed or ask for further material to justify the request. In order to ensure that JCs have a substantive role in issuing warrants, they must receive applications directly from requesting bodies and be provided with expert technical support to ensure a substantive assessment of warrants.[734]

Independent authorisation is required by human rights law

10. The ECtHR has stressed the importance of effective supervision of State surveillance by an independent judiciary. In *Klass v Germany* the Court made clear that, in an area where abuse is easy in individual cases and abuses have such harmful consequences for democratic society as a whole, it is desirable to entrust supervisory control to a judge: *"The rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and proper procedure".*[735] More recently in *Dumitru Popescu v Romania (no. 2)*,[736] the Court expressed the view that the body issuing authorisations for interception should be independent and that there must be either judicial control or control by an independent body over the issuing body's activity. Most recently and most pertinently the ECtHR ruled in *Roman Zakharov v Russia* that the Russian regime for interception violated Article 8. One feature highlighted by the Court was that while Russian law requires prior judicial authorization for interception measures, Russian judges in practice only apply purely formal criteria in deciding

[733] *Home Office v Rehman* [2001] UKHL 47.

[734] The explanatory notes say that Government will make tech expertise available to the IPC but there are no details and no particular obligations are provided on the face of the Bill. Explanatory Notes, p. 8, para. 13: The Investigatory Powers Commissioner will be able to draw on extensive legal and technical expertise. Guide to powers, p.31, para. 75: The IPC will oversee how the agencies use bulk personal datasets: "Supported by a team of Judicial Commissioners and technical and legal experts, the Commissioner will audit how the agencies use them and they will report publicly on what they find". 176: On how the JCs will be funded, and the Sec of State will provide staff, accommodation, equipment and 'other facilities' as necessary, after consultation with the IPC.
In the explanatory notes on 176 (p. 54, para 409): "It is intended that the resources afforded to the Investigatory Powers Commissioner will ensure that the office is fully staffed with judicial, official, legal and technical support to ensure that the Commissioners are fully able to perform their oversight and authorisation functions and to hold those that use investigatory powers to account".

[735] *Klass and others v Federal Republic of Germany*, European Court of Human Rights, 2 EHRR 214, 6 September 1978.

[736] No. 71525/01, § 61, 26 April 2007; 70-73, and cited with approval in *Case of Iordachi v Moldova*, 25198/02, 10 February 2009.

whether to grant an authorization, rather than verifying the necessity and proportionality of imposing such measures.[737] Strasbourg case law, taken together, is clear on the need for a fully independent body, with sufficient expertise and agency to engage in a review of the evidence put forward to justify a surveillance warrant.

A two-stage authorisation is unnecessary and risks delay.

11. This apparently and understandably concerns the Agencies. David Anderson reports, "*There was some resistance on the part of intercepting authorities to the idea of double authorisation, which was perceived as unnecessarily time-consuming."* He further reports that *"Most intercepting authorities did not mind whether their warrants were issued by the Secretary of State or by a judge, so long as a quick turnaround could be achieved and urgency procedures were in place*".[738]

12. In recognition of concerns that have been expressed regarding warrants that may have international relations ramifications, Liberty advocates for an amendment to the internal processes in place for MI6 which could require a certain category of warrants to receive internal approval by the Foreign Secretary before the formal authorisation process is triggered.

The sheer volume of surveillance warrants - set to increase under the expanded powers in the Draft Bill – is unsuitable for small number of Cabinet ministers.

13. This was the primary reason given by David Anderson for recommending judicial authorisation. He cited the "*remarkable fact (at least to an outsider) that the Home Secretary routinely signs thousands of warrants per year, most of them concerned with serious and organised crime and the remainder with national security."*[739] In 2014 the Home Secretary personally authorised 2345 interception and property warrants and renewals i.e. about 10 per working day. Liberty shares the Reviewer's concerns that this may not be the best use of the Home Secretary's time given her responsibility for a huge department of State. Removing primary responsibility from one individual who already bears huge responsibility for policing, immigration and other services, is supported by the reflections of a former Home Secretary, David Blunkett, who has written of his time as Home Secretary *"my whole world was collapsing around me. I was under the most horrendous pressure. I was barely sleeping, and yet I was being asked to sign Government warrants in the middle of the night. My physical and emotional health had cracked."*[740] Liberty also questions whether Ministers are best placed to decide the legality of warrants. In 2014 during an oral evidence session with the Intelligence and Security Committee, Phillip Hammond MP, the Secretary of State for Foreign and Commonwealth Affairs, appeared to misunderstand a number of key RIPA terms – in particular the distinction between internal and external communications – and appeared

[737] Roman Zakharov v Russia (47143/06) 4 December 2015, paragraph 263.
[738] David Anderson QC, A Question of Trust, paragraph 14.54
[739] David Anderson QC, A Question of Trust, paragraph 14.49.
[740] Blunkett: How I cracked under the strain of scandal, The Guardian, 7 October 2007, available at: http://www.guardian.co.uk/politics/2006/oct/07/uk.davidblunkett.

confused about how the warrant system for surveillance operates.[741] This is a cause for concern, given his huge, current, responsibility for authorising 8(4) RIPA warrants.

Arguments concerning Ministers' democratic or political accountability for surveillance warrants are misconceived and misplaced.

14. In its March 2015 report, the ISC concluded that Ministers should retain responsibility for authorising warrants: "*ministers, not judges, who should (and do) justify their decisions to the public*".[742] The Reviewer responded to this argument in his report in June by righty observing that ministers are not currently democratically accountable for their role in issuing warrants as disclosure of the existence of a warrant is criminalised and will remain under clause 43 and similar provisions of the Draft Bill.[743]

15. A corollary to this argument is that ministers are politically accountable for the Agencies and will be required to resign if things ever go wrong. This is also incorrect. While the Home Secretary is responsible for setting the strategic direction of the Government's counter-terrorism policy and the Cabinet Minister responsible for MI5, MI5 - like the police - is operationally independent. MI5's Director General retains operational independence for day-to-day decision-making. Historically, when terrorist attacks have tragically succeeded, this has not led to political resignations. Despite inquests and inquiries following the 7/7 attacks and the murder of Fusilier Lee Rigby uncovering internal errors in the Agencies' handling of information relating to those responsible for the attacks, this has not resulted in the 'political accountability' now being claimed. One significant error revealed in the ISC report into the murder of Lee Rigby was an Agency delay in requesting intrusive surveillance for one of the men convicted of the murder – without the delay, intrusive surveillance would have been in place in the weeks before the murder.[744]

16. In reality, oversight and accountability for Agency activities is instead provided by a patchwork of mechanisms – including public inquiries, the ISC, and legal challenges brought against the Government. Liberty believes there are many ways in which this oversight and accountability could and should be enhanced but it is not correct to argue that political accountability is provided by the ministerial sign off on warrants.

17. Against the background to the publication of the Draft Bill, whereby senior Ministers have colluded with Agency heads to grant and authorise intrusive powers that have not been granted by Parliament, the claim that Ministers provide 'democratic accountability' should be given short shrift. On the very day the Bill was published the Home Secretary announced that the Agencies had been secretly conducting bulk communications data surveillance on the entire UK population for the last ten years. Nick Clegg has described his astonishment when he and a handful of Cabinet Ministers were told of this by

[741] See, for example: http://www.theguardian.com/politics/2014/dec/11/philip-hammond-powers-warrants-understanding
[742] Paragraph 203GG.
[743] Clauses 43 & 44 of the Draft Bill continue to criminalise the disclosure of the existence of an interception warrant without authorisation to do so.
[744] For example, the ISC report into the murder of Fusilier Lee Rigby revealed a catalogue of administrative errors by the Agencies in handling information concerning the two men ultimately convicted of his murder. (paras 318-333).

officials in 2010.[745] Far from providing accountability, ministers have been complicit in keeping undemocratic secrets.

One-stage judicial authorisation is the norm in comparable jurisdictions.

18. In America,[746] federal investigative or law enforcement officers are generally required to obtain judicial authorisation for intercepting 'wire, oral and electronic' communications, and a court order must be issued by a Judge of a US District Court, US Court of Appeals or FISA judge. In Australia, law enforcement interception warrants must be issued by an eligible Judge or a nominated Administrative Appeals Tribunal judge.[747] In Canada it is unlawful to intercept private communications unless the interception is in accordance with an authorisation issued by a judge,[748] and in New Zealand police can only intercept a private communication in tightly prescribed circumstances, including requiring a warrant or emergency permit that can only be issued by a High Court Judge.[749] If the UK wants to be able to claim it is in a world class league for good practice in surveillance, it must at the very least adopt one-stage judicial authorisation.

Judicial authorisation would encourage co-operation from US tech firms.

19. The need for reform that guarantees true independence was pressed home to the Reviewer by the Silicon Valley tech firms who, given the US tradition for judicial warrants, feel uncomfortable with the UK model of political authorisation. These firms operate in a global marketplace and need to adhere to procedures fit for a world-leading democracy. The UK is alone among democratic allies in permitting political authorisation.

Recommendations

- Liberty believes there should be a one-stage surveillance authorisation process undertaken by a JC who is supported by technical experts and therefore is in a position to assess the application and accompanying evidence and make a reasoned decision as to the necessity and proportionality of the application sought.[750]
- IPC and JCs should be appointed by the Judicial Appointments Commission, as is the case for appointments to comparable Tribunals, and not directly by the Prime Minister. Prime ministerial appointment undermines the perception of independence and does not amount to 'world leading' oversight.
- The IPC should not have the power to unilaterally remove a JC.

---

[745] *Only 'tiny handful' of ministers knew of mass surveillance, Clegg reveals,* The Guardian, 5 November 2015, available at - http://www.theguardian.com/world/2015/nov/05/nick-clegg-cabinet-mass-surveillance-british-spying

[746] Under Title III of the *Omnibus Safe Streets and Crime Control Act 1968*, 18 U.S.C. §§ 2510-22, as amended by the *Electronic Communications Privacy Act* (ECPA) of 1986, the *Communications Assistance to Law Enforcement Act* (CALEA), by the *USA PATRIOT Act* in 2001, by the *USA PATRIOT Reauthorization Acts* in 2006, and by the *Foreign Intelligence Surveillance Act (FISA) Amendments Act* of 2008.

[747] *Telecommunications (Interception and Access) Act 1979*, section 39, as amended by the *Telecommunications Act 1997*. Note that Federal warrants relating to national security can be authorised by the Attorney General. See also the various States and Territories that have enacted legislation in order to make the Federal provisions applicable to State and Territory Police, see for example the *Telecommunications (Interception) (State Provisions) Act 1988* (Victoria).

[748] Canada *Criminal Code*, Part VI, section 186.

[749] Part 11A of the *Crimes Act*, and under the *Misuse of Drugs Amendment Act 1978*.

[750]

- If a JC refuses a request for interception, an appeal should lie with the IPC. This process should replace the provisions in the Draft Bill that allow the Secretary of State to simply make a fresh application to the IPC which has the effect of rendering a JCs powers illusory.
- The power to modify surveillance warrants should lie with a JC and not the Secretary of State.
- Judicial authorisation should be a pre-requisite for all surveillance requests including retention of and access to communications data, and warrants for encryption keys under Part III RIPA.
- Warrants should only be available for targeted and not thematic or mass surveillance. The scope of warrants permitted under the Draft Bill undermines the requirement for a necessity and proportionality assessment. "Thematic warrants" for hacking and interception and the provisions for bulk warrants in Part 6 are designed to licence surveillance on a disproportionate scale, placing those charged with issuing/reviewing warrants in the position of either impugning the fundamental aims of the legislative scheme, or accepting the highly dubious premise that routine, daily, surveillance of billions of communications can amount to a proportionate action.

Legal Thresholds for surveillance

20. The Draft Bill re-legislates for RIPA's three broad statutory grounds for issuing surveillance warrants. The Secretary of State may issue warrants for interception, hacking, communications data retention and acquisition and for the use of all bulk powers when he/she considers it necessary and proportionate: *"in the interests of national security", "for the purpose of preventing or detecting serious crime", or "in the interests of the economic well-being of the UK so far as those interests are also relevant to the interests of national security".* This final ground can apply only where it relates to the acts or intentions of persons outside the British Islands. Retention and acquisition of communications data can be authorised on many more grounds (see paragraph 25 below) and by many more public authorities.

21. All three main statutory grounds for authorising surveillance are unnecessarily broad and vague and left dangerously undefined. As the decision will continue to lie with the Secretary of State, the test will be met by whatever he or she subjectively decides is in the interests of national security or the economic well-being of the UK. This means that individuals are not able to foresee when surveillance powers might be used, and grants the Secretary of State a discretion so broad as to be arbitrary.

22. The three grounds contain no requirement for reasonable suspicion that an individual has committed or intends to commit a serious criminal offence, nor even suspicion or evidence that a serious crime has been or is going to be committed. This gives licence for speculative surveillance.

23. The national security ground is particularly problematic, as the Courts have responded with considerable deference to Government claims of 'national security', viewing them

not as a matter of law, but as executive led policy judgements.[751] National security as a legal test is therefore meaningless. The second ground is similarly broad and open-ended and the Government has not sought to clarify the circumstances in which 'national security' as opposed to 'the prevention and detection of serious crime" will be in play.

24. The use of broad and vague notions such as 'national security' and 'economic well-being' risks interference with political and other lawful activity that ought to go unimpeded in a democratic society. In an era when Members of Parliament have been labelled *"domestic extremists"* and when the Prime Minister has stated *"The Labour Party is now a threat to national security"* the continued undefined use of these terms in enabling legislation is not sustainable.

Recommendation

- Liberty believes that these grounds should more tightly defined on the face of the Bill and linked to the objective threshold of reasonable suspicion of criminality. A significantly higher level of specificity is required if these three grounds are to act as an effective check on the use of intrusive powers.

Communications data retention and acquisition

25. Parts 3 & 4 of the Draft Bill seek to re-legislate for the existing communications data retention and acquisition regime under RIPA and DRIPA but with an additional requirement for communications providers to generate and retain "internet connection records" and establish a Request Filter as previously proposed, and rejected, in the Draft Communications Data Bill, 2012.[752]

26. Part 4 gives the Secretary of State the power to issue a retention notice to require telecommunications operators to retain all communications data for up to twelve months. Communications data is defined as data which may be used to identify or assist in identifying the sender, recipient, time, duration, type, method, pattern, or fact of a communication, along with system used to make a communication, its location and the IP address or other identifier of any apparatus used. Part 3 grants a long list of public authorities the power to self-authorise access to communications data for a list of ten broadly defined purposes where it is necessary and proportionate for them to do so. As well as the three main grounds capable of justifying interception and hacking, these include – in the interests of public safety, for the purpose of protecting public health, assessing or collecting any tax, duty or levy payable to any government department,

[751] Lord Hoffman at para 50, *Secretary of State for the Home Department v Rehman* [2001] UKHL 47: Lord Hoffman has stated that whether something is 'in the interests' of national security "is not a question of law, it is a matter of judgment and policy" to be determined not by judges but to be "entrusted to the executive".

[752] Public authorities must operate a "single point of contact system". Authorisations will last for one month and can be renewed. Telecommunications operators must take reasonable steps to provide information requested. Where an authorisation under Part 3 relates to conduct outside the UK, any requirements or restrictions imposed by the law of the country in which the activity will take place may be considered when establishing whether the operator took reasonable steps to comply. The Bill would place a series of obligations on the telecommunications provider to protect the data, with a view to ensuring its integrity, protect it from deletion, and prevent unlawful or unauthorised access or disclosure. A telecommunications operator would not be permitted to disclose the existence of a notice. The duty to comply with a retention notice would only apply extraterritorially to the extent that there is a duty to have regard to the requirement or restriction.

exercising functions relating to the regulation of financial services and markets or financial stability, identification of the deceased, or assisting investigations into alleged miscarriages of justice.[753] Judicial authorisation is required only for local authority access to communications data and requests by public bodies for communications data in order to identify a journalist's source.[754] In all other cases, a senior officer within a public authority will grant an authorisation and in exceptional circumstances this person does not even need to be independent from the investigation. This largely mirrors the existing regime under DRIPA, RIPA and associated Orders.

27. Liberty supports the important role of communications data in missing persons situations, preventing and investigating serious crime. We do not believe however that the role of communications data in the investigation of crime justifies the *blanket* retention of the historic communications data of the entire population for 12 months. We also object to the lax access regime that currently exists under RIPA and is replicated in the Draft Bill. We do not believe an operational case has been made either for blanket ICR retention or The Request Filter and we believe that both proposals would violate human rights law.

Revealing nature of communications data

28. Communications data provides a detailed and revealing picture of somebody's life in the digital age. As defined under DRIPA and RIPA it can disclose the date, time, duration and type of communication, the type of communication equipment used, its location, the calling telephone number and the receiving telephone number. This can reveal personal and sensitive information about an individual's relationships, habits, preferences, political views, medical concerns and the streets they walk. As the CJEU has put it:

> *"those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."*[755]

29. In December 2013 US District of Colombia Judge Richard J Leon found that a lawsuit challenging the NSA's previous regime of bulk metadata collection demonstrated a "substantial likelihood of success"[756] and said of modern data metadata:

> *"I cannot imagine a more 'indiscriminate' and 'arbitrary invasion' than this systematic and high tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval…Surely, such a program infringes on 'that degree of privacy' that the founders enshrined in the Fourth Amendment."*

---

[753] Clause 46(7).
[754] Section 37 of the *Protection of Freedoms Act 2012* introduced a requirement for prior judicial authorisation for access to communications data by local authorities which is replicated in clause 59 of the Draft Bill. Clause 61 of the Draft Bill provides for judicial commissioner approval to identify or confirm journalistic sources.
[755] *Digital Rights Ireland (C-293/12) and Seitlinger and Others* (C-594/12).
[756] Klayman v Obama in the United States District Court for the District of Colombia, 16 December 2013, available at: http://apps.washingtonpost.com/g/page/world/federal-judgerules-nsa-program-is-likely-unconstitutional/668/.

30. The Government seeks to diminish the importance and sensitivity of communications data by distinguishing it from the content of communications. At one time a firm distinction between communications data and content would have been more credible, for example when much communication was by letter: everything inside the envelope is content, everything on the outside communications data. However, this distinction has been eroded by the scale of modern internet and mobile phone usage. As communications have become increasingly digital, the data generated is much more revealing and copious than before, allowing the state to put together a complete and rich picture of what a person does, thinks, with whom, when and where. Often, communications data can be of more use than content: it is expansive, easy to handle, analyse and filter; and, it tends to be collected in a consistent manner. In 2015 the ISC remarked: *"We were surprised to discover that the primary value to GCHQ of bulk interception was not in reading the actual content of communications, but in the information associated with those communications."*[757]

31. Indeed in many circumstances the picture of someone's life that can be created through examination of communications data will be more revealing than the content of may of their communications. As Stewart Baker, former senior counsel to the US NSA observed in 2013, metadata *"absolutely tells you everything about somebody's life. If you have enough metadata you don't really need content."*[758] The value of metadata and the use that the UK's closest ally is prepared to make of it was left beyond doubt following comments by the former head of the NSA, Michael Hayden in 2014: "*We kill people based on metadata*."[759] Furthermore, consider the range of situations in which just the fact of a single communication and the identity of the parties speaks volumes: the phone call from a senior civil servant to a reporter on a national newspaper immediately before a major whistle-blower scandal fills the front pages; the email to a civil liberties watchdog from a police officer during the course of an inquest into a death in police custody.

Regime incompatible with recent court judgments

32. We believe that the current retention and access regimes - let alone the proposal to impose further obligations on ISPs to generate and retain ICR data in the Draft Bill - violate human rights law and will be found in breach of the European Charter of Fundamental Rights and Freedoms, when the CJEU considers communications data retention and acquisition once again in 2016. In April 2014 the CJEU ruled in *Digital Rights Ireland* that the EU Data Retention Directive which mandated blanket data retention between 6 -24 months was invalid due to its sweeping interference with privacy rights.[760] The CJEU acknowledged the important role of data retention and access

[757] Intelligence and Security Committee, Privacy and Security: a modern and transparent legal framework, paragraph 80.
[758] Stewart Baker, quoted in David Cole, 'We Kill People Based on Metadata', New York Review of Books blog (10 May 2014), available at http://www.nybooks.com/blogs/nyrblog/2014/may/10/we-killpeople-based-metadata/
[759] General Michael Hayden, quoted in David Cole, 'We Kill People Based on Metadata', New York Review of Books blog (10 May 2014), available at http://www.nybooks.com/blogs/nyrblog/2014/may/10/we-killpeople-based-metadata/
[760] *Digital Rights Ireland (C-293/12) and Seitlinger and Others* (C-594/12).

for the prevention and detection of serious crime but laid out the following ten principles to ensure compliance with human rights standards –

1. restrict retention to data that is related to a threat to public security and in particular restrict retention to a particular time period, geographical area and / or suspects or persons whose data would contribute to the prevention, detection or prosecution of serious offences (paragraph 59);

2. provide exceptions for persons whose communications are subject to an obligation of professional secrecy (paragraph 58);

3. distinguish between the usefulness of different kinds of data and tailor retention periods to the objective pursued or the persons concerned (paragraph 63);

4. ensure retention periods are limited to that which is 'strictly necessary' (paragraph 64);

5. empower an independent administrative or judicial body to make decisions regarding access to the data on the basis of what is strictly necessary (paragraph 62);

6. restrict access and use of the data to the prevention, detection or prosecution of defined, sufficiently serious crimes (paragraphs 60-61);

7. limit the number of persons authorised to access and subsequently use the data to that which is strictly necessary (paragraph 62);

8. ensure the data is kept securely with sufficient safeguards to secure effective protection against the risk of abuse and unlawful access (paragraph 66);

9. ensure destruction of the data when it is no longer required (paragraph 67); and

10. ensure the data is kept within the EU (paragraph 68).

33. Three months after the judgment, the UK Government responded with emergency legislation – the *Data Retention and Investigatory Powers Act 2014* (DRIPA) - which was rushed onto the statute book in 7 days in July 2014. Prior to the decision in *Digital Rights Ireland*, senior courts across Europe had annulled domestic legislation seeking to implement the EU Directive– including Bulgaria[761], Romania[762], Germany[763], Cyprus and

[761] In 2008 the Bulgarian Supreme Administrative Court, found the legislation implementing the EU Data Retention Directive incompatible with the country's constitutional protection of personal privacy.

[762] In October 2008, the Romanian Constitution Court became the first to declare legislation transposing the EU Directive in breach of its Constitution. The Court found that the mandatory retention of communications data scheme engaged a number of fundamental rights, namely the right to freedom of movement, the right to intimate, family and private life, privacy of correspondence and the right to freedom of expression. In finding its transposing legislation disproportionate, the Court relied on, amongst other issues, the reversal of the ordinary presumption of innocence and the lack of a reasoned basis for the retention period required, finding also that retention on the scale required was 'likely to prejudice, to inhibit the free usage of the right to communication or expression'. Decision no 1258 of the Romanian Constitutional Court, 8 October 2009. Available at: http://www.legiinternet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decisionregarding-data-retention.html.

[763] In March 2010, Germany's Constitutional Court declared the provisions of its law transposing the Directive unconstitutional. In finding the communications data retention regime incompatible with constitutional protection for personal privacy, the Court commented that 'the protection of communication does not include only the content but also the secrecy of the circumstances of the communication, including if, when and how many times did some person…contact

the Czech Republic. Following the judgment, courts in a further six Member States, including five courts of final appeal, have relied on DRI in holding national data retention legislation invalid – including courts in Austria, Slovenia, Belgium, Romania, Netherlands, Slovakia.

34. Liberty is currently representing David Davis MP and Tom Watson MP in their legal challenge to DRIPA. In July 2015 the High Court upheld their challenge and struck down sections 1 & 2 DRIPA finding them incompatible with the British public's right to respect for private life and communications and to protection of personal data under Articles 7 and 8 of the EU Charter of Fundamental Rights. The High Court has found sections 1 and 2 of DRIPA unlawful on the basis that: they fail to provide **clear and precise rules to ensure data is only accessed for the purpose of preventing and detecting serious offences**, or for conducting criminal prosecutions relating to such offences; and: access to data **is not authorised by a court or independent body**, whose decision could limit access to and use of the data to what is strictly necessary. The ruling observes that: "*The need for that approval to be by a judge or official wholly independent of the force or body making the application should not, provided the person responsible is properly trained or experienced, be particularly cumbersome."*[764]

35. The Government appealed the judgment to the Court of Appeal. In November 2015 the Court of Appeal referred two questions to the CJEU, namely (1) Did the CJEU in Digital Rights Ireland intend to lay down mandatory requirements of EU law with which the national legislation of Member States must comply? And (2) Did the CJEU in Digital Rights Ireland intend to expand the effect of Articles 7 and/or 8 of the Charter beyond the effect of Article 8 ECHR as established in the jurisprudence of the ECtHR? On 4 May 2015 another CJEU reference on data retention post DRI was made by a higher court in Sweden asking whether a general obligation to retain traffic data covering all persons, all means of electronic communication and all traffic data without any distinctions, limitations or exceptions for the purpose of combating crime is compatible with EU law taking into account the Charter.[765] The outcome of these references will have significant bearing on the lawfulness of the Draft Bill.

Recommendations

- The Draft Bill should provide for a system of **targeted retention and acquisition which allows law enforcement bodies to request retention and acquisition of communications data for specific individuals on suspicion of serious criminality.** Liberty believes it would be feasible and desirable to construct a targeted

another. The Court went on to find that 'the evaluation of this data makes it possible to make conclusions about hidden depths of a person's private life and gives under certain circumstances a picture of detailed personality and movement profiles; therefore it can not be in general concluded that the use of this data presents a less extensive intrusion than the control of the content of communications. Bundersverfassungsgericht, 1 BvR 256/08. English press release at http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10- 011en.html (judgment only in German).

[764] Davis and Watson v SS Home Office, 17/7/2015 [2015] EWHC 2092 (Admin)

[765] Request for a preliminary ruling from the Kammarrätten i Stockholm (Sweden) lodged on 4 May 2015 — Tele2 Sverige AB v Post- och telestyrelsen
(Case C-203/15) available at - http://curia.europa.eu/juris/document/document.jsf?text=&docid=165124&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=1126567.

communications data retention and acquisition regime. Instead of the Secretary of State issuing speculative retention notices, law enforcement would be able to apply to a judge for retention and acquisition of communications data in an intelligence-led manner when investigating serious crime. The ten vague purposes for which data can be accessed should be replaced with a requirement for named individuals and reasonable suspicion of serious crime.

- Judicial authorisation – by the newly created tribunal of JCs – should be required for all public authority access to communications data. But in the case of privileged and confidential communications a stricter legal threshold for access should be met (see page 54).
- This scheme would have the benefit of complying with the DRI judgment, preventing further litigation and providing for a more effective and efficient communications data regime. The volume of communications data used in serious crime investigations is an infinitesimal fraction of that retained – at huge cost – on millions of innocent people. Just as the ECtHR judgment in *S and Marper* v UK[766] required a new policy on police retention of innocents' DNA so too does the CJEU judgment in DRI require a new policy on the retention of innocents' communications. In response to *S and Marper* the Government legislated for a new policy and has undertaken the deletion of over 1 million DNA profiles. Yet no attempt has been made to explain or justify the different approach it has taken here.

Internet connection records

36. The Draft Bill describes a new category of information – an internet connection record – and provides significant new powers (a) for the Home Secretary to require telecommunications operators to generate and retain 'internet connection records' (ICRs) for up to 12 months and (b) for a multitude of public authorities to gain access to ICRs. Under current legislation in DRIPA 2014, public telecommunications operators may be required to retain "*relevant communications data"* for up to 12 months[767], including data which may be used to identify the internet protocol (IP) addresses of senders and recipients of communications. However, this specifically excluded the obligation to retain the most revealing data, previously described as 'web logs' but presented here as ICRs, that would explicitly identify the websites or internet communications services users have accessed.[768]

37. ICRs are defined in the Bill as "*the internet protocol address, or other identifier, of any apparatus to which a communication is transmitted for the purpose of obtaining access to, or running, a computer file or computer program".*[769] In explanatory notes accompanying the Bill, ICRs are described as "*a record of the internet services that a specific device connects to – such as a website or instant messaging application – captured by the company providing access to the internet".*[770]

38. A plethora of public authorities will have access to ICRs, including HMRC, the Department for Work and Pensions (and a range of other government departments), NHS Trusts, the

[766] *S and Marper v United Kingdom* [2008] ECHR 1581.
[767] *Data Retention and Investigatory Powers Act 2014,* section 1
[768] *Counter Terrorism and Security Act 2015,* section 21(3)(c)
[769] *Draft Investigatory Powers Bill 2015,* clause 71, subsection (9)(f)
[770] *Draft Investigatory Powers Bill 2015: Explanatory Notes,* p.29

Gambling Commission, the Food Standards Agency, and several ambulance services.[771] The scale of public authority access to ICRs mirrors that for communications data, barring local authorities who will not be granted access.

39. Public authorities will not need a warrant to obtain an individual's detailed internet connection records. Applications by law enforcement and public authorities to acquire ICRs relating to suspects will mirror existing provisions for access to communications data and instead be authorised by a 'designated person'[772] within the public authority, and then by a 'single point of contact.'[773]Provisions in the draft Bill would permit law enforcement and public authorities to gain access to ICRs for three purposes: to identify who or what device has sent a communication or used an internet service; to identify what internet communications services have been used, when and how; and to identify when and where a person has accessed or made available illegal material.[774]

Defining ICRs

40. ICRs do not naturally exist within the technical infrastructure of a telecommunications operator. The draft Bill failed to define the exact fields of information that would constitute an 'internet connection record'. The Home Office's accompanying ICR factsheet says that ICRs "*will involve retention of a destination IP address but can also include a service name (e.g. Facebook or Google) or a web address (e.g. www.facebook.com or www.google.com) along with a time/date*".[775] Therefore, in practice, an ICR will comprise identifying connection information, likely to include client and server IP addresses, port connections, time, DNS (Domain Name System) logs, and possibly MAC addresses.

41. "*The voice of the internet industry*", the Internet Service Providers Association (ISPA) has expressed concern that ICRs have not been properly defined.[776] In a recent meeting between ISPA members and the Home Office, civil servants were still unable to define the fields of information that would constitute an ICR.[777] This indicates a failure to identify exactly what data is necessary for the stated purposes, and what data retention would be excessive.

42. In practice, ICRs would provide a detailed record of internet connections for every person in the UK and comprise a 12 month log of websites visited, communications software used, system updates downloaded, desktop widgets used (e.g. calendars, notes), every mobile app used (e.g. Whatsapp, Signal, Google Maps), and logs of any other device connecting to the internet, such as games consoles, baby monitors, digital cameras and e-book readers.

43. Law enforcement bodies can currently obtain similarly extensive internet connection data for specific surveillance targets in several ways. First, they can request

---

[771] *Draft Investigatory Powers Bill 2015,* schedule 4, part 1
[772] *Draft Investigatory Powers Bill 2015,* clause 46
[773] *Draft Investigatory Powers Bill 2015,* clause 60. A SPoC is an "*accredited*", "*trained*" individual. *Investigatory Powers Bill: Explanatory Notes,* 4 Nov 2015, p. 27
[774] *Draft Investigatory Powers Bill 2015,* clause 47
[775] *Factsheet*: *Internet Connection Records,* Home Office, 4 Nov 2015
[776] *Internet industry has major concerns on the Investigatory Powers Bill,* ISPA Conference press release, 19 Nov 2015
[777] *Home Office Meeting re IPBill* by Adrian Kennard, 25 Nov 2015 – http://www.revk.uk/2015/11/home-office-ipbill.html

telecommunications operators to retain the data of specific targets on a forward-looking basis.[778] Secondly, they can request retrospective 'internet connection' data on specific targets from operators who temporarily store it for their own business purposes.[779] Thirdly, if they are seeking to prevent or detect serious crimes (such as child sex abuse, financial crime, drug smuggling, etc.) they can request data or assistance from GCHQ, which has a remit to provide intelligence for these purposes.[780] Intelligence sharing to tackle online child sexual exploitation will be fortified by the establishment of the NCA and GCHQ Joint Operations Cell (JOC), which was launched in November 2015[781].

44. Liberty believes the case supporting this expanded data collection by ISPs, including its claimed benefit to law enforcement, is deeply flawed, contradicted by the available evidence, and has been accurately described as "*overstated and misunderstood*".[782] Further, there is no other known Five Eyes country in which operators have been or are being forced to retain similar internet connection data[783]. In fact, David Anderson noted that "*such obligations were not considered politically conceivable by my interlocutors in Germany, Canada or the US*", and therefore, "*a high degree of caution*" should be in order[784]. As the CJEU ruled in 2014[785], the indiscriminate collection and storage of communications data is a disproportionate interference with citizens' right to privacy. It is unacceptable that Government is attempting to bypass this ruling, and to extend its policy of blanket data retention.

45. Access to ICRs will be granted for the furtherance of one of three purposes. However, the need for further powers in relation to each of these purposes is flawed.

Rebuttal to Purpose 1: Identifying the individual device that has sent a communication online

46. The Metropolitan Police and National Crime Agency (NCA) have suggested that without ICRs, they cannot resolve IP addresses (that is, identify web users) and continue investigations in a minority of cases (approximately 14%[786]).

47. In the *Operational Case for the Retention of Internet Records*, published with the draft Bill, three case studies of discontinued investigations relating to child sexual exploitation and three relating to fraud are presented to support the argument for retaining ICRs. It is claimed that ICR retention would be required in order to progress those investigations and increase chances of accurately identifying a web user.[787] However, the likelihood of bulk ICRs to prove vital in accurately identifying otherwise anonymous suspects of

[778] *Draft Investigatory Powers Bill 2015: Explanatory Notes,* p.25
[779] *Operational Case for the Retention of Internet Connection Records,* 2015, p.25
[780] *The threat from serious crime* – GCHQ, 2015 http://www.gchq.gov.uk/what_we_do/the-threats-we-face/the-threat-from-serious-crime/Pages/index.aspx
[781] *GCHQ and NCA join forced to ensure no hiding place online for criminals* – NCA, 6 Nov 2015
[782] *Written evidence regarding Investigatory Powers Bill* – Adrian Kennard (Andrews & Arnold Ltd.), 25 Nov 2015, http://www.me.uk/IPBill-evidence1.pdf
[783] *A Question of Trust: Report of the Investigatory Powers Review* – David Anderson Q.C., June 2015, p.265
[784] Ibid
[785] *Digital Rights Ireland* (C-293/12) *and Seitlinger and Others* (C-594/12), 8 April 2014
[786] It is argued that the retention of ICRs would improve the chances of being able to resolve an IP address in 14% of cases in a sample from the US based National Centre for Missing and Exploited Children, NCMEC - as cited in the ICR evidence base: *Operational Case for the Retention of Internet Connection Records,* 2015, p.14
[787] *Operational Case for the Retention of Internet Connection Records,* 2015, p.20

serious crime has been questioned by ISPs and technologists.[788] The justification relies on the assumption that online criminals offend using a regular browser or public file sharing service on their own device, using personal internet connections, without employing the most basic of the widely available anonymity tools to avoid detection. The use of privacy-enhancing and anonymising tools such as Virtual Private Networks (VPNs), which securely 'tunnel' internet connections; Tor, a secure browser that anonymises users' location and identity; and proxy web browsers that bypass filters and anonymise web browsing, is widespread and increasing exponentially. ICRs will be unusable and in fact misleading where such privacy tools have been used. Furthermore, the retention of ICRs will push internet traffic, both legitimate and otherwise, into more protected spaces. This inevitable digital shift will render ICRs an invasive database of, almost exclusively, innocent citizen's digital lives, and forced retention of them a costly, out-dated, ineffective strategy.

48. In the limited cases where the ICRs might assist in resolving an IP address they will provide limited assistance in identification of suspects as they can only help to identify a device, such as a laptop or PC – not an individual user. Identifying a specific user requires a context of information that would typically be gathered in a targeted surveillance operation. Devices such as laptops, PCs, tablets and even smart phones are commonly shared within families, workplaces and public institutions, further diminishing the value of bulk ICRs in identifying an individual suspect. Indeed, ICR data is "inexact and error-prone".[789]

49. In evaluating the efficacy of ICRs in serving the purpose of IP resolution and identification of a suspect, we are informed by the case study of Denmark's Data Retention Law (*Logningsbekendtgørelsen*), effective 2007-2014, which required communication service providers to retain internet session logs. Denmark's data retention law compelled telecommunications operators to store internet session data for 12 months including client and server IP addresses, port numbers, transmission protocols and timestamps.[790] The data retention excluded DNS logs (i.e. the names of the websites the server IP addresses corresponded to). **A self-evaluation report published by the Danish Ministry of Justice in December 2012 found that several years of collecting internet session data had not yielded any significant benefits for law enforcement - session data had played a minimal role in only one case.**[791] In fact, Ministry staffers reported that session logging "*caused serious practical problems*" due to the volume and complexity of the data hoarded.[792] In 2013, approximately 3,500 billion telecommunication records were

---

[788] *Written evidence regarding draft Investigatory Powers Bill* – Adrian Kennard (Andrews & Arnold Ltd.), 1 Dec 2015, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25065.html

[789] *Written evidence regarding draft Investigatory Powers Bill* - Tim Panton, 1 Dec 2015, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25104.html

[790] *Logningsbekendtgørelsen 2006* (https://www.retsinformation.dk/forms/r0710.aspx?id=2445). An English translation produced by the Ministry of Justice is available at https://itpol.dk/sites/itpol.dk/files/TFR40200.pdf

[791] *Redegørelse om diverse spørgsmål vedrørende logningsreglerne* – Justitsministeriet, Dec 2012 (http://www.ft.dk/samling/20121/almdel/reu/bilag/125/1200765.pdf). There is no English translation. The article "*In Denmark, Online Tracking of Citizens is an Unwieldy Failure*" - TechPresident, 22 May 2013, discusses the report (http://techpresident.com/news/wegov/23918/denmark-government-will-not-allow-ordinary-citizens-have-digital-privacy).

[792] Ibid.

retained in Denmark, averaging 620,000 records per citizen.[793] In June 2014, the Danish government repealed the obligation on operators to retain session data on the basis that it was "*questionable whether the rules on session logging can be considered suitable for achieving their purpose*".[794]

Rebuttal to Purpose 2 - identify what ISPs an identified suspect has used, when and how[795], in order to inform law enforcement as to which communications service providers to request further information from.

50. The second part of the Home Office's case for mass ICR retention rests on the idea that this is required to help inform law enforcement request further information on identified suspects. This argument overlooks the range of intrusive powers already on the statute book. It is far more preferable, from both a human rights and law enforcement perspective, to employ robust targeted powers on identified suspects than intrude on the rights of the entire population. Existing powers for obtaining further information about communications of suspects include: using targeted interception, making targeted requests for communications data from service providers, and seizing and forensically examining a device. However, the Home Office presents these targeted approaches as less favourable than the mass retention of ICRs.

51. The argument in favour of this new, invasive category of bulk data retention rests, in part, upon the claim that there is an "*extremely high threshold*"[796] and "*very limited circumstances in which the interception of communications content can be authorised*", and therefore targeted interception "*cannot be used in most law enforcement cases*".[797] This is a peculiar argument, as interception is used for three broad statutory purposes: the prevention and detection of serious crime (which accounts for 68% of interception warrants[798]), the interests of national security and for the economic well-being of the UK.[799] The case studies provided to support the case for ICR retention all qualify as serious crimes[800], for which interception can be used, as they relate to child sex abuse, fraud and human trafficking.

52. Additionally, it is claimed that law enforcement bodies cannot request data from popular online service providers who store communications data for their own purposes, such as Facebook, without ICR evidence proving that the individual or device in question definitely accessed their service.[801] Without this data, they argue that such a request "*is unlikely to be necessary and proportionate*".[802] Liberty does not recognise this explanation. If the authorities have objective and reasonable grounds for suspecting

---

[793] *Written evidence on Investigatory Powers Bill: Technology Issues* - IT-Political Association of Denmark, 2 Dec 2015, p.2
[794] *Justitsministeren ophæver reglerne om sessionslogning ("The Ministry of Justice repeals the rules about session logging*) – Justitsministeriet, 2 June 2014, http://www.justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2014/justitsministeren-oph%C3%A6ver-reglerne-om-sessionslogning
[795] *Draft Investigatory Powers Bill 2015,* clause 47 (4)(b)
[796] *Operational Case for the Retention of Internet Connection Records,* 2015, p.17
[797] *Operational Case for the Retention of Internet Connection Records,* 2015, p.16
[798] *HM Government Transparency Report 2015: Disruptive and Investigatory Powers,* p.34
[799] *Draft Investigatory Powers Bill 2015,* clause 14 (3)
[800] Serious crimes are those that incur a sentence of 3 years or more; violent crimes; crimes involving substantial financial gain, or conduct by a large number of persons in pursuit of a common purpose. *Draft Investigatory Powers Bill 2015,* clause 195 (1),
[801] *Operational Case for the Retention of Internet Connection Records,* 2015, p.4; p.25
[802] *Operational Case for the Retention of Internet Connection Records,* 2015, p.4

serious criminality and further believe that the suspect's use of a telecommunications platform may have furthered/provide evidence of the offence a request for communications data will be necessary and proportionate.[803] If the suspect did not use the communications service, the data will simply not be there to obtain.

53. As a third argument for ICR retention, law enforcement bodies say it is "*thanks to seizure of devices*" that it has thus far been possible to identify communications services used by suspects, but that seizure of a device "*will not always be the preferred course of action in an investigation, as it is an overt action that will normally involve an arrest*"[804]. Investigators would rather "*develop intelligence on the group covertly*" and establish any possible "*previous linkages"* between group members. However, links between group members can be covertly discovered through a targeted communications data retention order; through requests for retrospective data from the operators who store it for their own purposes; or through interception.

54. The value of ICRs in consistently and accurately identifying what internet communications services a suspect or suspected victim has used and when has been over-estimated and misunderstood. In an ICR Factsheet produced by the Home Office, it is claimed that ICR retention would identify what communications services a person has used and when, and thus "*allow the police to determine whether a missing person was using a particular smartphone app or social media website prior to his or her disappearance".*[805] Similarly, in a recent Home Office meeting to discuss the concerns of the Internet Service Providers Association (ISPA), civil servants claimed ICRs could help police discover when a missing person last accessed a communications service such as Twitter on a smart phone. In response, "*ISPA members immediately pointed out the huge flaw in this argument*".[806] ICRs may not accurately show *when* communications services have been used, and therefore are not helpful for informing an accurate time frame for further communications data requests. This is because communications software (especially on smartphones) often stays connected in the background whether in current use or not, remaining connected for a period of days, weeks or months[807]. Connection records show connection timestamps rather than access timestamps, and one such 'internet connection' could exceed the 12 month retention period by the time it is logged. ISPs and technologists have expressed serious concern that the Home Office has based an extensive, invasive data collection policy on a fundamental misunderstanding, or worse misguidance, as to how internet connections work, and has provided misleading descriptions of what purposes ICRs will serve accordingly.

Rebuttal to Purpose 3 - to "identify the accessing of illegal online services or websites"[808].

---

[803] Indeed, many online public services are co-operative with law enforcement: Facebook, for example, co-operates with the NCMEC and has an established system for law enforcement data requests[803]. In the period January 2015 – June 2015, UK law enforcement made 3,384 requests to Facebook alone for various types of data, relating to 4,489 accounts; Facebook found legal basis to comply with 78.04% of these requests[803].

[804] *Operational Case for the Retention of Internet Connection Records,* 2015, p.17

[805] *Factsheet*: *Internet Connection Records,* Home Office, 4 Nov 2015

[806] *Home Office Meeting re IPBill* by Adrian Kennard, 25 Nov 2015 – http://www.revk.uk/2015/11/home-office-ipbill.html

[807] The main transmission protocol used online, TCP, can maintain a connection for hours, days, or even years; whilst protocols such as SCTP and MOSH aim to keep a connection active indefinitely, even with changes to IP addresses at each end or changes in connection.

[808] Draft Investigatory Powers Bill 2015, clause 47 (4)(c).

55. The value of ICRs in consistently and accurately identifying access to illegal websites has also been over-estimated and misunderstood. The bulk collection of ICRs raises concerns about inaccurate and possibly incriminating representations of innocent individuals' internet use.

56. Each 'internet connection' involves the exchange of multiple packets of data. Some of these packets of data relate to the scripts, images and styles that constitute various elements of a webpage. An image or video embedded on a webpage may be hosted elsewhere and generate a separate 'internet connection', which may relate to a server the individual had no intention, or even knowledge, of accessing. Similarly, it is unlikely that ICRs will be able to distinguish between a webpage visited out of an individual's own volition and a pop-up. Bulk ICR retention could be exploited by hackers for nefarious purposes – for example, by embedding 'suspicious' scripts into webpages, or spamming individuals with suspicious pop-ups. In addition, many browsers and apps pre-cache links – that is, store data from linked webpages before they are even visited by the user, to improve access speed if it is selected. Clearly, bulk ICRs collected on a population-wide scale will lead to misleading, inaccurate and potentially suspicious information as to innocent internet use.

Threat to privacy and security posed by bulk retention of ICRs

57. The population's detailed internet connection records will be collected and stored by ISPs. This has generated significant concern among ISPs and the public alike, as this new trove of extremely valuable data will be attractive to criminal hackers and difficult to protect. When a similar plan to collect 'web logs' was proposed in 2012, the **Joint Committee on the Draft Communications Data Bill concluded that it would create a "*honeypot for casual hackers, blackmailers, criminals large and small from around the world and foreign states*"[809].** In their final report, the Joint Committee noted that *"storing web log data, however securely, carries the possible risk that it may be hacked into or may fall accidentally into the wrong hands, and that, if this were to happen, potentially damaging inferences about people's interests or activities could be drawn"*[810]. This wealth of data in the wrong hands could be used for identity theft, scamming, fraud, blackmail, and even burglaries, as connection records can show when internet access occurs in or out of the house, representing a daily routine. This is an unacceptable level of risk to inflict on innocent internet users. At a time when the UK is plagued by prolific hacks (e.g. TalkTalk, Vodafone, Vtech), taking the title as the most hacked country in Europe and the second most hacked in the world,[811] it is extraordinarily irresponsible to coerce private companies with the burden of generating, storing and securing vast swathes of revealing data on the general public. Companies are unable to guarantee protection of the customer information they already have – entrusting them with new data of unprecedented volume and value will have disastrous effects for the UK's internet industry and the safety of British internet users. In addition to the obligation on UK telecommunications operators, the draft Bill places a duty on overseas operators to

[809] MPs call communications data bill 'honeypot for hackers and criminals' – Alan Travis, The Guardian, 31 Oct 2012.
[810] Joint Committee on the Draft Communications Data Bill: Report, 11 Dec 2012, pp.28-29
[811] Internet Security Threat Report, 2015 – Symantec, http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Symantec_annual_internet_threat_report_ITU2015.pdf. Reported on in, British companies bombarded with cyber attacks – Sophie Curtis, The Telegraph, 14 April 2015.

collect and retain ICRs on UK citizens.[812] This creates an extra set of concerns for UK citizens' privacy and the protection of extremely revealing data in other jurisdictions. The UK Government's general insistence on extraterritorial application of bulk communications data retention powers sets a "*disturbing precedent*" for other, more authoritarian countries to follow, as Anderson pointed out in his independent review.[813]

58. The difficulty of tracking some online criminals is a real problem. However, it is not a problem that mass surveillance programs – least of all this one - can solve. Bulk ICR retention will not be able to meet these three investigative purposes with greater efficacy than usual targeted surveillance methods for investigations; in fact, it could easily cause false suspicion. Arguably, the £175 million budgeted to fund reluctant telecommunications operators to spy on their customers would be better spent on hiring more officers to conduct targeted, warranted surveillance on suspects of serious crime.

Recommendations

- Liberty believes that clause 71 (9)(f) should be removed from the Bill, and mass internet connection record retention in any form should be wholly rejected.
- Explore and produce more information on the law around access to targeted communications data and the threshold for intercept. As this system is not currently subject to judicial oversight it may be the case that requests are being refused in circumstances where the legal threshold has been made out. A system of judicial authorisation of communications data requests would help ensure uniformity and the furtherance of investigations in circumstances where the requirements of necessity and proportionality are made out.

The Request Filter

59. The Draft Bill contains provisions for a communications data 'Request Filter[814]' – a feature previously proposed in almost identical terms in the draft Communications Data Bill. The Request Filter is a search mechanism, allowing public authorities to conduct simple searches and complex queries of the databases that telecommunications operators are required to build and hold. The Joint Committee on the Draft Communications Data Bill described the 'Request Filter' proposed in that Bill as "*a Government owned and operated data mining device*"[815], which significantly positions the Government at the centre of the data retention and disclosure regime. Access to the Filter, and the data it produces, would be subject to the same self-authorisation process as all communications data (see paragraph 25). In practice, the 'Request Filter' would be a search engine over a "*federated database*"[816] of each and every citizen's call and text records, email records, location data, and now internet connection records, made available to hundreds of public authorities.

60. The Government is keen to portray the Request Filter as a 'safeguard' that "*will minimise the interference with the right to privacy".*[817] However, the processing of personal data

[812] Draft Investigatory Powers Bill 2015, clause 79
[813] A Question of Trust: Report of the Investigatory Powers Review – David Anderson Q.C., June 2015, p.207
[814] Draft Investigatory Powers Bill 2015, clause 51
[815] Joint Committee on the Draft Communications Data Bill: Report, 11 Dec 2012, para. 113, p.35
[816] Ibid.
[817] Draft Investigatory Powers Bill 2015: Explanatory Notes, p.23

represents a significant privacy intrusion. Whilst a useful tool for complex data searches, the 'Request Filter' cannot be viewed as a straightforward safeguard. Rather it is a portal with power to put together a comprehensive picture of each of our lives. It raises many of the same concerns as a large and centralised store, with added security concerns of protecting multiple distributed databases.

61. Public authorities' permanent ability to access to the 'Request Filter' makes it an enticing and powerful tool that could be used for the broad range of statutory purposes - recently declared unlawful by the High Court.[818] The ability to conduct complex queries could increase the temptation to go on 'fishing expeditions': that is, to sift data in search of 'relationships' and infer that any concurrences are meaningful. This was one of the many concerns about this proposal expressed by the Joint Committee on the Draft Communications Data Bill.[819]For example, given this power, authorities could use communications data to identify attendees at a demonstration and correlate this with attendance at other public or private locations in the 12 month period; or to identify those regularly attending a place of worship, and correlate this with access to online radio websites, inferring risk.[820] Thus, this new ability could risk casting undue suspicion on thousands of innocent citizens.

62. Allowing hundreds of public authorities direct access to sensitive databases complicates the issue of protecting such stores (for example, stores of internet connection records). The duty to "*put in place and maintain an adequate security system"*[821] outlined in the draft Bill is clearly resides with the Secretary of State, but there is no information available as to what that security system would be.

Recommendations

- Liberty's primary concern is the indiscriminate collection, generation, and storage of billions of items of data on innocent citizens. Liberty believes that Article 8 requires that individuals' privacy should not be interfered with unless there is clear reason to suspect crime, and as such, expansive distributed databases of innocents' communications are unlawful. Liberty believes that further processing personal data, without judicial authorisation and for purposes unconnected with serious crime would constitute a further unjustified interference with Article 8 rights.

Targeted interception

63. Powers for "targeted interception" of communications are contained in Part 2 Chapter 2 DIPB. There are three types of warrant – a "targeted warrant", a "targeted examination warrant" which permits the examination of domestic communications intercepted via Part 6 bulk interception powers, and a "mutual assistance" warrant which would be granted to an international partner who requests assistance under mutual legal assistance treaty. A targeted interception warrant can be issued by Secretaries of State (and in certain circumstances by Scottish Ministers[822]) on application by the intelligence

[818] Davis and Watson v SS Home Office, 17/7/2015 [2015] EWHC 2092 (Admin).
[819] Joint Committee on the Draft Communications Data Bill: Report, 11 Dec 2012, para. 126, p.37
[820] GCHQ appears to practice similar data mining on the basis of supposed risk factors: Profiled: From Radio to Porn, British Spies Track Web Users' Online Identities – Ryan Gallagher, The Intercept, 25 Sept 2015.
[821] Draft Investigatory Powers Bill 2015, clause 53 subclause (5)
[822] See clauses 17 & 18; where the application relates to persons or premises reasonably believed to be in Scotland.

services, the National Crime Agency, London Met, PSNI, PSS, HMIC and the Chief of Defence Intelligence subject to the weak judicial review process (discussed at paragraphs 1- 18). Warrants can be issued on the three main grounds (which replicate existing RIPA grounds). The Draft Bill provides for each warrant to last a minimum of six months – whereas under RIPA, serious crime warrants last three months.

Thematic warrants

64. The most radical departure from the scheme under RIPA relates to the scope of interception warrants. RIPA clearly provided that warrants for targeted interception were required to name "*one person as the interception subject*" or "*a single set of premises*".[823] Clause 13 of the Draft Bill radically reforms this requirement and prescribes that warrants may cover "*a particular person or organization or a single set of premises*" or "*a group of persons who share a common purpose or who carry on, or may carry on, a particular activity* " or "*more than one person or organization, or more than one set of premises, where the conduct authorized or required by the warrant is for the purposes of the same investigation or operation*" or for the maintenance or development of interception apparatus and training. This allows warrants to be issued in respect of people whose names are not known or knowable when the warrant is sought. This is confirmed by clause 23 which provides that a thematic warrant must describe the relevant purpose or activity and name or describe as many of those persons as is reasonably practicable. The creation of thematic warrants in the Draft Bill means that "external" communications intercepted in their billions under Part 6 could be trawled thematically for groups sharing a common purpose or carrying on a particular activity. It provides for an open-ended warrant that could encompass many hundreds or thousands of people. The expansive scope of these warrants, combined with the broad grounds for which they can be authorised do not impose sufficient limits on the authorities' interception powers.

65. This change follows the dramatic disclosure in March 2015 that the Secretary of State is already issuing "thematic" interception warrants. The ISC reported that the significant majority of 8(1) warrants relate to one specific individual, but that some don't apply to named individuals or specific premises but rather groups of people. The current Home Secretary has apparently derived the authority to do so from the broad definition given to "person" found elsewhere in RIPA, despite the unequivocal reference to "one person" in section 8(1). Liberty does not recognise this unorthodox statutory construction and any thematic warrants that have been issued under this power are likely to be *ultra vires.* Like much surveillance practice in recent years, this appears to be a case of the Agencies and Executive claiming powers well beyond those provided on the face of RIPA and other enabling statutes. The existence of "thematic" warrants also represents a huge departure from the position at common law which has long banned "general warrants". The ISC reported that the Interception of Communications Commissioner has "*made some strong recommendations about the management of thematic warrants*" and has in some cases recommended that they are cancelled.[824] The ISC has expressed further *"concerns as to the extent that this capability is used and the associated safeguards.*

[823] Section 8(1)(a) RIPA.
[824] ISC report, paragraph 45.

Thematic warrants must be used sparingly and should be authorised for a shorter timescale than a standard 8(1) warrant"[825]

66. Liberty believes the scope of warrants permitted under clause 13 fails to comply with both common law and ECHR standards. In Zakharov v Russia[826] where the ECtHR found Russia's interception scheme in violation of Article 8 of the Convention, the Court cited the fact that Russian '*courts sometimes grant interception authorisations which do not mention a specific person or telephone number to be tapped, but authorise interception of all telephone communications in the area where a criminal offence has been committed.'* [827] While thematic warrants do not relate to geographical location, they are sufficiently broad to violate Article 8 and need considerable amendment on the face of the Draft Bill.

Bar on admissibility of intercept material in criminal justice system

67. Clause 42 maintains the section 19 RIPA bar on admissibility of interception material in criminal trials and Inquiries Act 2005 proceedings. There is not justifiable reason for maintaining the bar on intercept admissibility. The first consequence of lifting the ban would be an increase in successful prosecutions for serious offences. The latest Privy Council review into the issue which reported in December 2014 concluded that a properly funded use of intercept material as evidence may result in a "*significant increase in the number of successful prosecutions*."[828]

68. Removal of the ban will also ensure that criminal defendants rights are not breached in cases where interception has formed part of the investigation. The ECtHR has ruled that failure to disclose intercept evidence in certain circumstances will breach Article 6 ECHR.[829] Furthermore the current ban has fuelled a corruption of domestic fair trial standards and abusive counter-terrorism laws, from control orders to TPIMs, to the corrosive growth of Closed Material Procedures across our justice system.

69. The Agencies have previously sought to block the admissibility of intercept on grounds that it would reveal sensitive methods or subject their activities to too great a scrutiny. In this new post-Snowden age of transparency, this argument cannot hold. Further the existence of public interest immunity certificates and mechanisms to protect sensitive information will easily be able to protect matters which are genuinely sensitive. If material obtained by bugging, interception by foreign authorities and – under the terms of the Draft Bill - hacking can be made admissible, there is no logical or coherent case for excluding intercept. As a last resort, the authorities also always have the option of abandoning a particular prosecution. Successive Government initiated reviews over the past two decades have concluded that intercept should be made admissible. The only remaining objection from the Agencies now seems to be on cost grounds. No doubt the requirement to transcribe and disclose intercept evidence would impose an additional burden on the authorities – as do all requirements to ensure that the criminal process is effective, efficient and just. But it would only be material which fulfills the test for

[825] ISC report, page 24 recommendation D
[826] (47143/06) 4 December 2015.
[827] Paragraph 265.
[828] See Intercept as Evidence, December 2014, Page 23.
[829] *Natunen v Finland* (Application no. 21022/04).

disclosure to a defendant at trial – material capable of undermining the case for the prosecution – which need be disclosed.[830] Given the current volumes of interception it would likely be only an infinitesimal fraction, and could have the salutary effect of focusing the authorities' minds on the primacy that should be given to criminal investigations, prosecutions and trials over speculative, intelligence gathering fishing expeditions.

Recommendations

- Liberty believes that the scope of targeted interception warrants needs to be significantly curtailed to prevent speculative and abuse interception and comply with the recent ECtHR judgment in *Zakharov v Russia.*
- Liberty also calls for clause 42 to be deleted from the Draft Bill so that material obtained by interception can be made admissible in criminal trials and inquiries under the Inquiries Act 2005.

Targeted hacking

70. Part 5 of the Draft Bill makes provision for "targeted hacking" euphemistically termed "equipment interference" in the Bill. There are two types of warrant: "targeted equipment interference warrants" and "targeted examination warrants", the latter of which can be issued in relation to material obtained via the bulk hacking powers in Part 6. Secretaries of State (and in certain circumstances Scottish Ministers[831]) can issue both types of warrants to the intelligence agencies and the Chief of Defence Intelligence where he or she considers it necessary and proportionate on the three main grounds. In contrast to the scheme for interception, the power to issue hacking warrants is also extended to chief constables, deputy chief constables, assistant chief constables and senior HMRC officers on application from junior HMRC and police officers 'for the purpose of preventing and detecting serious crime'.[832] In making their determination, chief constables are required to consider whether the warrant's objectives could reasonably be achieved by other means. Ministers are under no such obligation. Warrants last for six months and can be renewed potentially indefinitely. Warrant applications will be subject to the weak system of judicial review discussed elsewhere in this document. Warrants can be modified by ministers without the approval of a JC and modification can include changing the name, descriptions and scope of the warrant. Chief constables are required to have their decisions to modify warrants reviewed by a JC.

71. A hacking warrant authorises a person to interfere with any equipment for the purpose of obtaining "communications", "private information" and "equipment data".[833] "Communications" can comprise speech, music, sound, visual images, *data of any*

[830] Section 3 of the Criminal Procedure and Investigations Act 1996.
[831] Clause 86.
[832] The majority of police forces can only hack devices and networks with a "British Isles connection" (although NCA has global powers) and this requirement is made out if any of the conduct, equipment interfered with or private info sought is in the British Islands.
[833]Equipment data is defined at clause 82.

description and any form of signal between two individuals, two machines or between a person and a machine. Private information is defined to include any piece of information relating to a person's private or family life. This could include information stored on a device or a network which hasn't been communicated. Communications and private information can be obtained by *"monitoring, observing or listening to a person's communications or other activities and recording anything that is monitored, observed or listened to".*[834]

72. Hacking is prima facie unlawful as a matter of domestic criminal law[835] and before 2015, hacking was not avowed as an intelligence agency or law enforcement capability. This only changed in February 2015 when the Home Office published a consultation on a Draft Code of Practice for Equipment Interference in response to Privacy International and others' claim in the IPT concerning the hacking disclosures contained in the Snowden documents. This Code referred only to the intelligence agencies and did not make reference to police hacking powers which were not officially acknowledged until the publication of the Draft Bill.

73. There is currently no clear or accessible legal framework governing the hacking of electronic devices and networks making current use of the practice likely unlawful on grounds that it is not in accordance with law to comply with the requirements of the HRA. Government claims the Agencies' hacking powers derive from broad and vague enabling powers contained in sections 5 and 7 of the *Intelligence Services Act 1994*.[836] Yet the enabling power bears no resemblance to the power now contained in the Draft Bill and the legislation pre-dates the powerful electronic hacking capabilities now utilised.

74. Police apparently derive hacking powers from section 93 of the Police Act 1997[837] yet when the head of the Metropolitan Police's Technical Unit gave oral evidence to the Draft Bill Committee he seemed unsure as to legal basis for the Met's powers.[838] Section 93 similarly bears no resemblance to the powers now contained in the Draft Bill and even as recently as 2010, when the related Code of Practice on "*Covert Surveillance and*

[834] Clause 81(4).

[835] Section 1 of the Computer Misuse Act 1990 makes it an offence to cause a computer to perform any function with intent to secure access to any program or data held within it if the access is unauthorised. Section 3 of the 1990 Act also makes it an offence to do any authorised act in relation to a computer if the intention is to impair its operation, hinder or prevent access to any program or data, to impair the operation of any program or reliability of data. Section 10 provides that section 1 has effect without prejudice to the operation of any enactment relating to the powers of inspection, search or seizure, but this carve out does not apply to section 3.
However, with their practices thrown into the light by Snowden's whistleblowing, the Government sought to immunise the intelligence agencies and amended the Computer Misuse Act 1990 to exempt, presently and retroactively, GCHQ from criminal culpability (*Serious Crime Act 2015*, Section 44).

[836] Section 5 covers activity in the UK and provides that a warrant authorised and issued by the Secretary of State may make lawful any "*entry on or interference with property or with wireless telegraphy* The ISC report sheds some further light on current practice. While the number of section 5 warrants obtained by the Agencies in 2013 is not disclosed, the report reveals that while the majority of warrants are targeted, a percentage were 'thematic' permitting the Agencies to use the same technique on multiple occasions or authorised 'IT Operations'.

[837] Under section 93 police can obtain authorisations for - "the taking of such action, in respect of such property in the relevant area, as [the authorising officer] may specify" and "the taking of such action in the relevant area as he may specify, in respect of wireless telegraphy".

[838] Oral evidence to the Draft Investigatory Powers Bill Committee, 16 December 2015, Detective Superintendent Paul Hudson, Head of Metropolitan Police Service Technical Unit.

Property Interference" was issued it referred only to physical property interference and not electronic hacking. Despite this, in a potentially explosive admission before the Draft Bill committee, the Metropolitan Police representative disclosed that equipment interference is used in a "majority" of serious crime cases. Over the past few years, various media outlets have sought to investigate hacking by the police. The Times and Sky News[839] have reported that the Met has purchased and begun using "IMSI catchers" and when the Hacking Team (a private company offering hacking services to Governments worldwide) was recently itself hacked it was revealed that the Met, NCA and Staffordshire police had shown interest in their products before apparently getting cold feet.[840] Until the publication of the Draft Bill the Met had adopted a NCND approach to hacking.

Highly intrusive nature of hacking

75. Hacking is potentially much more intrusive and damaging than any other forms of traditional surveillance such as bugging, interception and acquisition of communications data. Hacking can grant access to a large amount of highly sensitive data that has never been communicated or transmitted and gives the hacker access to all historical and future data stored on a device. Perhaps most uniquely it also grants the hacker total control over a device – phones and computers can be turned on or off, have their cameras or microphones activated, files added or deleted. Furthermore, all this can be done without the fact of the hack being known or knowable to the target.

76. The potential for intrusion is intensified in the digital age, when computers and mobile devices have replaced and consolidated our filing cabinets, photo albums, video archives, personal diaries and journals, address books, correspondence files and landline telephones. Increasingly these devices are also replacing our formal identification documents as well as our bank and credit cards. Devices may contain not only details about the user's personal circumstances (age, gender, or sexual orientation), but also financial information, passwords, privileged legal information and so on.

77. When malware is deployed, there is often a risk of contagion, both overseas and at home. This was dramatically demonstrated by the Stuxnet virus, believed to be an American-Israeli cyberweapon, which intended to hack a single Iranian uranium enrichment facility but infected energy giant Chevron among many other companies as well as Microsoft PCs around the world[841]. The risks of hacks spreading 'in the wild' cannot be overstated: Professor of Security Engineering at Cambridge University, Ross Anderson wrote to the Science and Technology Select Committee, "*it is only a matter of time before interference with a safety-critical system kills someone*"[842]. There is also the risk that hacks can malfunction, with severe consequences for critical infrastructures and

[839] Fake mobile phone towers operating in the UK, 10 June 2015, available at - http://news.sky.com/story/1499258/fake-mobile-phone-towers-operating-in-the-uk.
[840] UK Police tried to buy Hacking Team's Spytech leaked emails show, Vice News, 15 July 2015, available at - https://news.vice.com/article/uk-police-tried-to-buy-hacking-teams-spy-tech-leaked-emails-show
[841] *Obama Order Sped Up Wave of Cyberattacks Against Iran* – David E. Sanger, The New York Times, 1 June 2012
[842] *Written evidence regarding draft Investigatory Powers Bill* – Prof. Ross Anderson, 1 Dec 2015, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25159.html

even international relations. For example, Snowden revealed that NSA hacking malfunctions were responsible for the outage of Syria's internet in 2012[843], which may have caused simultaneous flight-tracking issues, and led government and opposition forces to erroneously blame each other for the incident[844].

78. Given the potential damage to computer security and corresponding vulnerability to criminal elements that results from hacking, the use of this technology poses clear risks to those it is used against in a way that engages many more rights than traditional forms of communications surveillance. Parliamentarians may also want to consider the cost of widespread hacking by the authorities. Hacks maintain and create permanent vulnerabilities which can then be further exploited by criminal elements raising the potential for hacking to be counterproductive in the fight against serious crime. Cybercrime already costs the UK £34bn per year, and these proposed powers seem certain to ensure that this cost rises.

Thematic hacking warrants

79. Clause 83 provides for thematic hacking warrants which amount to general warrants to hack groups or types of individuals in the UK. Hacking is not restricted to equipment belonging to, used by or in possession of particular persons. Instead the subject matter of warrants can target equipment "*belonging to, used by or in the possession of a particular organisation*" or "*persons who form a group that shares a common purpose or who carry on or may be carrying on a particular activity*" or more than one person or organisation "*where the interference is for the purpose of the same investigation or operation."* A hacking warrant can further authorise hacking "*equipment in a particular location*" or "*equipment in more than one location, where the interference is for the purpose of the same investigation or operation*" or "*equipment that is being, or may be being used, for the purposes of a particular activity or activities of a particular description*" as well as testing or maintaining capabilities. In addition the Draft Equipment Interference Code of Practice permits the targeting of people who are "not of intelligence interest".[845] It is difficult to foresee a more enabling and open-ended framework of the scope of domestic hacking capabilities. Hacking is by its nature much more prone to collateral intrusion than traditional forms of surveillance. ISMI catchers can for example pick up stored content of all mobile phones in a particular area. If use of the capability is to stand a chance of meeting the UK's human rights obligations, it is even more imperative that the legal framework for hacking requires specificity of targets.

Use of hacking material as evidence in the justice system

80. As hacking by its nature requires the alteration of content on a target device or network, it also raises new questions concerning the potential for electronic surveillance to undermine the integrity of a device or material located on a device that may later be sought to be used in evidence. There is presently no specific regulation of the use of

[843] *The Most Wanted Man in The World* – James Bamford, Wired, Aug 2014
[844] *Internet Shutdown Reported Across Syria* – Anne Barnard & Robert Mackey, The Lede: The New York Times Blog, 29 Nov 2012
[845] Draft Code of Practice on Equipment Interference (February 2014), Home Office.

hacking product in criminal trials.[846] The present position at common law is that the prosecution are under a duty to disclose all material in their possession or that they have inspected which may reasonably be considered capable of undermining the case against the defendant. Following the scandal concerning the non disclosure of the identity of undercover police officers during the trial of Ratcliffe-on-Soar protesters, that principle now extends to material relating to the manner in which evidence is obtained where such material might support and argument that its acquisition has resulted in unfairness or abuse. The Rose Report into the Ratcliffe-on-Soar Power Station Protest found that the CPS and the police had together failed to discharge the prosecution's disclosure duties.[847] In recognition of the unique potential of hacking capabilities and to avoid future miscarriages of justice and collapsed trials, the Draft Bill should contain specific proposals to ensure audit trails and police disclosure where prosecutions result from investigations that utilise hacking capabilities.

Recommendations

- Targeted hacking should be subjected to much stricter safeguards than other forms of electronic surveillance given the unprecedented level of intrusion, the harm to device and network security and the risk of damage to evidence that is inherent to the capability.
- Hacking warrants should be authorised only by JCs and only on the application of the intelligence agencies and chief constables, in keeping with the proposed framework for interception. Hacking requests should not be available to all police constables as currently provided in the Bill.
- Hacking warrants should only be granted where a JC is satisfied that the objectives of the warrant cannot be achieved by other less intrusive means.
- Hacking warrants should specify named individuals or premises. Thematic warrants aimed at particular locations or activities of a particular description should be removed from the Draft Bill.

---

[846] As Archbold explains - "*Neither the Police Act 1997 nor the 2000 Act purports to deal with the question of the admissibility of evidence obtained under their provisions"* (Chapter 15, paragraph 207).

[847] The police's disclosure obligations are set out in section 3 of the Criminal Procedure and Investigations Act 1996. The prosecution are to disclose all material, either in the prosecution's possession or inspected by the prosecution in connection with the case, which "might reasonably be considered capable of undermining" the case against the defendant. Unused material is required to be disclosed if, and only if, it satisfies this test; unused material which does not fulfil this test need not be disclosed to the defence. As Archbold explains: *"Material may assist the case for the accused not only where it could be used to explain the accused's actions, support his case, or provide material for cross-examination of prosecution witnesses, but also where it might support submissions that could lead to the exclusion of evidence, a stay of proceedings, or a finding that any public authority had acted incompatibly with the accused's rights under the ECHR (see the Attorney-General's guidelines, ante, at paras 10 to 14; and see R. v. Barkshire [2012] Crim.L.R. 453, CA, as to the duty to disclose material that might support an application for a stay based on entrapment)."*So it includes not only material which the prosecution may have seen which is capable of suggesting that the defendant did not commit the crime (or capable of attacking the credibility of prosecution witnesses, for example), but also material, for example, relating to the manner in which the evidence was obtained, where such material might support an argument that its acquisition has resulted in unfairness or abuse. This last principle was established in one of the cases that related to Mark Kennedy, where the CPS had failed to disclose the fact of Kennedy's surveillance (which involved taking contemporaneous notes and covert recordings of the protestors in the alleged preparation and commission of the offences). This would have had the capacity to show that he had acted as an agent provocateur and thereby entrapped those convicted.

- Hacking capabilities allow the authorities complete control over devices and the power to delete, alter or create stored content or communications, often leaving no trace of their actions. In the absence of robust safeguards concerning how hacking powers may be used, they present a grave threat to the integrity of electronic evidence, with corresponding implications for the fairness of trials and the safety of convictions. There should be mandatory requirement to record in a verifiable manner all action taken in relation to a device or network for each individual hack that takes place. There should be an absolute prohibition, backed up by criminal sanction, on creating, altering or deleting content on a hacked device beyond what is necessary to effect the hack. Liberty is deeply alarmed by recent disclosures that the police and Agencies have started hacking devices and networks in the absence of statutory authority and despite the lack of safeguards currently in place to protect against evidence tampering. We believe this has serious implications for the integrity of the UK's criminal and civil justice systems.

- Hacking warrants should be granted for a shorter duration than other forms of surveillance in recognition of the acute security implications of hacking.

Mass surveillance

81. Part 6 of the Draft Bill places the breathtakingly broad mass surveillance powers revealed by Edward Snowden and additional bulk surveillance practices on an explicit statutory footing. New powers to intercept, in bulk, 'external' communications (including vast swathes of domestic communications) and to acquire records of the entire nation's communications data are supplemented by powers permitting "industrial scale exploitation" [848] (GCHQ's own words) of electronic devices and networks. Part 7 further extends blanket surveillance powers away from a focus on the population's communications and towards the acquisition and linking of all public and private sector personal data databases.

Bulk interception

82. The intelligence agencies bulk interception programmes were disclosed for the first time by Edward Snowden in June 2013. They have never been debated or voted for by Parliament. The power to conduct mass interception has instead been inferred by GCHQ from the vaguely worded power in section 8(4) of RIPA. In a radical departure from common and human rights law principles, bulk warrants may be targeted at a telecommunications system or entire populations rather than specific, individual persons or premises as required under section 8(1) RIPA. This approach is maintained in clause 106 of the Bill. Bulk interception results in billions of communications being intercepted each day without any requirement of suspicion or even any discernable link to a particular operation or threat. Liberty understands that the Agencies are currently handling 50 billion communications per day. To place this in context there are only 7 billion people in the world and only 3 billion with access to the internet. The ISC reports that at the end of 2014, there were just 20 section 8(4) warrants in place authorising the vast volume of interception under this power.

[848] *How the NSA Plans to Infect 'Millions' of Computers With Malware* – Ryan Gallagher & Glenn Greenwald, The Intercept, 12 March 2014

83. Part 6 Chapter 1 provides for the intelligence agencies to conduct bulk interception of "external communications". At first glance, the mass interception these powers permit appears targeted at overseas communications. However, whilst the main purpose of a bulk interception warrant must be to collect "overseas-related" communications or CD, this includes communications where either the sender or recipient is in the UK but their correspondent is not. Internet based communications have further eradicated the distinction between external and internal communications. As first disclosed through Liberty and other NGOs litigation against the Government[849], the ISC has recently confirmed that Government considers that an "external communication" occurs every time a UK based person accesses a website located overseas, posts on a social media site overseas such as Facebook, uses overseas cloud storage or uses an overseas email provider such as Hotmail or Gmail. Searches on Google are counted as an external communication.

84. Material collected under a bulk interception warrant can be examined in accordance with "specified purposes" written into the warrant. The only guidance the Bill provides as to what these purposes may cover is a requirement that it must be more than simply e.g. "the interests of national security", but that "general purposes" will suffice.[850] The lack of guidance around what can amount to "specified operation purposes" means that the concept offers little practical protection and could in theory be as broad in its nature as the three grounds on which the warrant was originally justified.

85. While the criteria for selection cannot be "referable to an individual known to be in the British Isles at that time" where "the purpose of using those criteria is to identify the content of communications sent by, or intended for, that individual"[851] it is likely that for the vast majority of communications intercepted, the Agencies will have no knowledge as to where the senders and recipients are located. If it later becomes apparent that a target is in the UK (even if they have, in fact, been here all along) that process of selection and examination can continue for 5 days with only the requirement of an authorisation from a senior official. It seems likely that there will be many cases in which it will be unclear where an individual is currently located. The high threshold of 'knowing' that somebody is in the UK, will allow for widespread examination in cases where there is an element of doubt about an individual's current whereabouts. If examination would be in breach of the weak prohibition in clause 119 outlined above, the relevant agency can apply for a targeted interception warrant to examine the material anyway.[852]

86. Liberty, along with partner NGOs has lodged a challenge to the practice of mass interception under 8(4) RIPA at the ECtHR. The case was communicated in November 2015. Whilst the central question of the legality of the UK's bulk external interception regime is yet to be resolved, in *Liberty v UK* (2008), the ECtHR that the system for external interception under the pre-RIPA legislation that allowed interception to cover *'such external communications as are described in the warrant'* violated Article 8. The case concerned 'external communications' interception by the Ministry of Defence of

[849] https://www.liberty-human-rights.org.uk/sites/default/files/Witness%20statement%20of%20Charles%20Farr%20on%20behalf%20of%20the%20Intelligence%20Services%2016th%20May%202014.pdf#original
[850] Draft Investigatory Powers Bill, clause 111.
[851] Draft Investigatory Powers Bill, Clause 119(4).
[852] Draft Investigatory Powers Bill, Clause 12.

Liberty's telephone, fax and email communications between 1990 and 1997 and the violation allowed the interception of almost all external communications transmitted by submarine. The replacement RIPA framework for 'external interception' now subject to challenge is worded almost identically, as is the power in clause 106(4)(a) of the Draft Bill.

Bulk communications data acquisition

87. On the day that the Draft Bill was published, the Home Secretary announced that since 2005 the Agencies have been acquiring in bulk the communications data of the UK population under the vaguely worded section 94 of the *Telecommunications Act 1984.*[853] This had never previously been publicly admitted by the Executive and was apparently only known by a handful of Cabinet ministers.[854] Parliamentarians had previously been led to believe that communications data retention and acquisition by the Agencies took place under RIPA and DRIPA as the legislation specifically permits the Agencies to acquire communications data on national security and serious crime grounds.

88. By contrast with bulk interception, where a half-hearted attempt is made to tie surveillance to "overseas" communications, acquisition has as its main purpose the acquisition of data held by UK based companies. The power also purports to have extraterritorial effect.

Bulk hacking

89. The use of targeted hacking by the Agencies was only very recently acknowledged by Government through the publication by the Home Office of an Equipment Interference Code of Practice although it made no mention of bulk hacking capabilities. The scope of a bulk equipment interference warrant under the draft Bill is astonishingly broad, paving the way for intrusions over and above those revealed by Snowden, pinpointing hacking as the modus operandi of our expanding surveillance state. As with bulk interception, the main (but not sole) aim of the warrant must be to facilitate the obtaining of overseas data, but this does not prevent data on UK residents being collected as a subsidiary objective, or in pursuit of the main aim.[855] A bulk hacking warrant can authorise interference with any equipment whatsoever, for the purposes of obtaining communications, private information and equipment data or anything else connected with equipment mentioned in the warrant.[856] Bulk warrants can be issued in the interests of national security, economic wellbeing, or for the prevention and detection of serious crime.[857]

90. The Bill draws a broad overarching distinction – within the vast body of data which can be collected from a bulk hack – between "protected material" and other data. Broadly speaking, protected data is private information and the content of communications. A targeted warrant is required for the examination of protected data obtained under a

[853] Secretary of State for the Home Office the Right Honourable Theresa May, Oral Statement on publication of the Draft Investigatory Powers Bill, 4 November 2015 - https://www.gov.uk/government/speeches/home-secretary-publication-of-draft-investigatory-powers-bill
[854] http://www.theguardian.com/world/2015/nov/05/nick-clegg-cabinet-mass-surveillance-british-spying
[855] *Draft Investigatory Powers Bill 2015,* Clause 135(1)(c)
[856] *Draft Investigatory Powers Bill 2015,* Clause 135(4)(a)(iv)
[857] *Draft Investigatory Powers Bill 2015,* clause 137

bulk hacking warrant selected by reference to "an individual known to be in the British Isles at the time". However if data is not selected by reference to those criteria it can be examined without a targeted warrant. This does not prevent the examination of the communications or personal information of those in this country in the pursuit of broader objectives, or in order to access communications data. Where it later transpires that an individual who forms the focus for the selection of protected material is in the UK (even if he was there all along),all that is required to continue the process of examination for five days is the authorisation of a senior official. Non-protected data is everything not considered above. Equipment data and any other information connected with equipment which is not a communication or private information can be accessed without any additional authorisation.

91. The Home Office says that "*bulk equipment interference*" has been practiced under the Intelligence Services Act 1994[858], which allows for interference with property or "wireless telegraphy"[859]. Under this law, intelligence services can acquire a warrant to search a property or intercept a person's phone calls. There is no mention in the Act of bulk or mass equipment interference. However, under these out-dated Acts, British intelligence agencies have conducted intrusive, destructive and disturbing mass hacks, such as hacking the largest SIM manufacturer in the world to enable interception of millions of users' calls.[860] The Intelligence Services Act 1994 was written prior to the technological revolution of the past twenty years and cannot be considered a lawful basis for the mass hacking of technologies that were not even conceivable at the time of the Act's writing. Indeed, the Snowden documents revealed that British intelligence agencies expressed concern that their mass hacking practices "*may be illegal.*"[861] [862]

Bulk hacking - a significant expansion of power

92. The "Guide to powers" accompanying the draft Bill makes clear that bulk hacking is a significant step beyond conventional and surveillance powers, remarking that bulk equipment interference "*is used increasingly to mitigate the inability to acquire intelligence through* ***conventional bulk interception*** *and to access data from computers which* ***may never otherwise have been obtainable****" (emphasis added).*[863] Labelling mass interception powers as "conventional" when it is this Bill that for the very first time avows them makes a mockery of our parliamentary democracy. It also demonstrates the apparently insatiable demand from the security services to have unbridled access to all information. This is particularly concerning in light of the broad definition of equipment in the Bill. The draft Bill defines "*equipment"* as "*equipment producing electromagnetic, acoustic or other emissions or any device capable of being used in connection with such equipment*"[864]. This is unfathomably open-ended and could even include cars and

[858] *Draft Investigatory Powers Bill 2015: Guide to Powers and Safeguards,* pp.20-21
[859] *Intelligence Services Act 1994,* Section 5
[860] *The Great SIM Heist* – Jeremy Scahill & Josh Begley, The Intercept, 19 Feb 2015
[861] *UK Perspective on MIKEY-IBAKE*, Sept 2010, p.3 (https://www.documentcloud.org/documents/1077367-uk-perspective-on-mikey-ibake.html)
[862] As recently as April 2013, GCHQ was reluctant to extend deployment of QUANTUM malware due to "legal/policy restrictions": *Legal Issues UK Regarding Sweden and Quantum,* (https://www.documentcloud.org/documents/894386-legal-issues-uk-regarding-sweden-and-quantum.html)
[863] *Draft Investigatory Powers Bill 2015: Guide to Powers and Safeguards,* pp.20-21
[864] *Draft Investigatory Powers Bill 2015,* clause 149 (1).

aircraft, leaving the power open to potential abuses not just by future UK governments, buy by other states that will follow our lead in legislation.

Bulk hacking - Indiscriminate and speculative

93. Bulk hacking is by its nature indiscriminate, as acknowledged by the Draft Bill's Explanatory Notes: "*bulk equipment interference is not targeted against particular person(s), organisation(s) or location(s) or against equipment that is being used for particular activities".*[865] Instead, systems, services and software that have been carefully constructed to provide security are intentionally corrupted to impose the eyes and ears of the intelligence agencies on every phone call, text message and web click. In the offline world, granting this power would mean allowing secret services to break into and bug every house, leaving broken windows[866] for anyone else to get in but all without the individual whose house it is knowing this has happened. In the digital world, even more rich and revealing data can be gathered as computers and mobile devices have taken the place of our filing cabinets, diaries, calendars, video archives, photo albums, book shelves, address books and correspondence files. Furthermore, this digital forced entry does not only entail intrusion into highly personal spaces, but control over them. For example, spies can alter, add or delete files, send messages, turn devices on or off, or covertly activate cameras and microphones. As demonstrated by GCHQ's OPTIC NERVE program[867], this could literally mean subverting millions of webcams into covert home surveillance cameras. Such extraordinary power over the private lives of citizens fundamentally alters the relationship between citizen and state, and will breed distrust in law enforcement while having potentially significant repercussions for the Rule of Law. In human rights terms, such sweeping and speculative powers can never meet a test of necessity and proportionality.

Security repercussions of bulk hacking

94. Bulk hacking critically **damages the security** of complex modern technologies upon which modern society is built. The Five Eyes intelligence agencies find security flaws in software and stockpile them for later 'equipment interference', rather than inform developers so that they can be fixed or responsibly dealt with.[868]As such, mass hacking goals prevent intelligence agencies from protecting the public's cybersecurity. President Obama's Review Group of Intelligence and Communications Technologies criticised this approach, concluding: "*In almost all instances, for widely used code, it is in the national interest to eliminate software vulnerabilities rather than to use them for US intelligence collection. Eliminating the vulnerabilities – 'patching' them – strengthens the security of US Government, critical infrastructure, and other computer systems."*[869] Furthermore,

---

[865] *Draft Investigatory Powers Bill 2015: Explanatory Notes*, p. 83

[866] A US intelligence official described state hacking using a similar analogy: *"You pry open the window somewhere and leave it so when you come back the owner doesn't know its unlocked, but you can get back in when you want to".* Quoted in, *U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show* – Barton Gellman & Ellen Nakashima, 30 Aug 2013

[867] In which several millions of Yahoo users' webcam calls were intercepted to take and store images for a facial recognition program. *Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ* – Spencer Ackerman & James Ball, The Guardian, 28 Feb 2014 (http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo).

[868] *Mind-blowing secrets of NSA's security exploit stockpile revealed at last* – Shaun Nichols, The Register, 4 Sept 2015

[869] *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies,* 12 Dec 2013, p. 220

the UN Group of Governmental Experts (UN GGE) recently released a consensus report, recommending that states "*should seek to prevent the proliferation of malicious ICT and the use of harmful hidden functions*"[870]. Although the alarm has been raised on the danger of stockpiling exploits, this Bill would proliferate the practice and in fact boost the market for exploits to be created and sold. In addition, security vulnerabilities created or stockpiled by British intelligence agencies can also be exploited by foreign intelligence agencies or any non-state actors who discover them. ,An explicit British bulk hacking law will set a disturbing precedent for other, more authoritarian states to follow and join a cyber-arms race.

95. "*Bulk equipment interference"* is an especially excessive, dangerous and destructive power designed to achieve international mass surveillance by any means. If passed, this and other bulk powers will gradually eradicate private spaces from modern society whilst damaging national security. Bulk hacking is one of the most objectionable powers in the draft Bill, jeopardising human rights in the present and future.

Bulk Personal Datasets

96. Part 7 provides the Agencies with powers to acquire 'bulk personal datasets' (BPDs). This power does not currently exist. BPDs are essentially databases held either by the private or public sector and are defined in the Draft Bill by reference to their nature "as *a set of information that includes personal information relating to a number of individuals* where the *nature of the set is such that it is likely that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service."* [871]They cover manual and electronic records. Personal data is given a broad definition – it has the same meaning as the *Data Protection Act 1998* but also includes data relating to deceased individuals and data is defined to include 'any information which is not data'. Private misuse of a bulk dataset will be an offence, subject to up to 12 months imprisonment.

97. Acquisition, retention and examination of these databases will be governed by a warrant system similar to that for bulk interception and bulk hacking. Warrants are issued by the Secretary of State on application from the three Agencies and the process mirrors the framework in place for warrants for other bulk powers in Part 6. Judicial involvement is limited to the flawed judicial review model. "Class warrants" concern applications for *descriptions* of personal data – so presumably 'health data' or 'travel data', for example. Under the terms of the Bill, this is the default type of BPD warrant. 'Specific bulk warrants' can be applied for (a) where the requesting agency wants to request a bulk dataset that doesn't fall within a class described in a class BPD warrant or (b) where it does fall within a class warrant but where the intelligence agency at any time considers that it would be "appropriate" to seek a specific BPD warrant. Specific BPDs will presumably apply to the most sensitive type of databases – such as mental health hospital data, or patient identifiable FGM data. Applications must include a descriptions of the bulk personal dataset to which it relates and an explanation of the operational purposes for which the intelligence service wishes to examine it. Specific BPD warrants may also authorise obtaining, retaining and examining bulk personal datasets that do not

[870] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* – UN GGE, 22 July 2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174
[871] Draft Investigatory Powers Bill, Clause 150

exist at the time the warrant is issued but may "reasonably be regarded as replacements" for the a dataset that has been sought.

98. Agencies' acquisition of BPDs was only finally avowed by the ISC in March 2015. In its report, the ISC disclosed limited information about BPDs:

"Bulk Personal Datasets may relate to the following types of information:

a. i)***;

b. ii)***;

c. iii)***;

d. iv)***

e. v)***"

And that, "As of mid-2014:

f. SIS held *** Bulk Personal Datasets;

g. MI5 held ***; and

h. GCHQ held ***"

99. As regards the content and nature of BPDs, the ISC set out that:

"*These datasets vary in size from hundreds to millions of records. Where possible, Bulk Personal Datasets may be linked together so that analysts can quickly find all the information linked to a selector (e.g. a telephone number or *) from one search query."*[872]** And the datasets "***may include significant quantities of personal information about British citizens***".[873] Apparently "*None of the Agencies was able to provide statistics about the volume of personal information about British citizens that was included in these datasets*".[874] The Director General of MI5 has also cryptically explained to the ISC: *"there are datasets that we deliberately choose not to reach for, because we are not satisfied that there is a case to do it, in terms of necessity and proportionality."*[875]

Sensitive information is apparently held in the datasets including an individual's religion, racial or ethnic origin, political views, medical condition, *, sexual orientation, or any legally privileged, journalistic or otherwise confidential information**.[876] The ISC notes in passing that the Agencies **may share the datasets with overseas partners**.[877] Each Agency reported that they had disciplined – or in some cases

[872] ISC report, para 156.
[873] ISC report, para 158.
[874] ISC report, footnote 142.
[875] ISC report, para 162.
[876] ISC report, para 163.
[877] ISC report, para 163.

dismissed – staff for inappropriately accessing personal information held in these datasets in recent years.[878]

100. The acquisition of bulk private and sensitive data on the UK population by the intelligence agencies is a new and radical development. There is currently no legal authority for the Agencies to acquire these datasets. As the ISC diplomatically put it "*the rules governing the use of Bulk Personal Datasets are not defined in legislation*".[879] Government further claims that BPDs may be acquired by using investigatory powers – which means that Government believes it can use surveillance capability, such as hacking or interception to obtain mass data sets from a private company or public body. It also hints that it buys mass datasets from the private sector.[880]

101. **No argument is even attempted that BPDs are necessary or proportionate for Article 8 HRA purposes.** The ISC reported that the Agencies told them that BPDs are an 'increasingly important investigative tool' to 'enrich' information obtained through other techniques and concludes that BPDs are 'relevant' to national security investigations. "Enriching" and "relevant" does not meet the legal threshold for lawfulness.

Recommendation

- Part 7 should be removed from the Bill. There is no operational case for the Agencies to collect, process and link personal data on the entire UK population. It is in principle a deeply offensive proposition. Current law allows data to be transferred across the private and public sector to further national security and the prevention and detection of crime. The Agencies therefore already have gateway powers to obtain information on those it identifies as being subjects of interest.

Are bulk powers necessary?

102. While Liberty supports the use and value of targeted intrusive surveillance powers, we believe that the mass speculative interception of communications; retention and acquisition of communications data; bulk hacking and bulk personal dataset acquisition is unlawful, unnecessary and disproportionate.

103. The Government has not really attempted to make an operational case for bulk surveillance. The bulk powers are presented in the draft Bill as "*crucial to monitor known and high-priority threats"* and also as "*a vital tool in discovering new targets and identifying emerging threats".*[881] In his July report, David Anderson offered six anecdotes provided by the Agencies in an attempt at justifying mass interception. However, with the vague and limited information provided, it is impossible to assess whether the security outcomes could have been achieved by using the wealth of targeted and operation-led intrusive surveillance powers at the Agencies' disposal. In nearly all of the examples, reference is made to known terrorists or a specific "intelligence operation".

[878] ISC report, para 163.
[879] ISC report, para 157.
[880] Guide to Powers and Safeguards, para 71.
[881] Guide to powers, p.20 para. 33

104. The available evidence indicates that mass surveillance powers have not been effective in tackling serious crime, especially not terrorism. Rather, there is evidence that mass surveillance practices impede law enforcement efforts. Bulk telephone data has not proved useful for counterterrorism in the U.S.. The Privacy and Civil Liberties Oversight Board, an independent executive branch board in the U.S., found that the bulk telephone records program conducted under Section 215 of the USA Patriot Act not only raised constitutional and legal concerns, but had no material counterterrorism value:

> *"Based on the information provided to the Board, including classified briefings and documentation, we have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack.*[882]

105. Similarly, the President's Review Group on Intelligence and Communications Technologies concluded in 2013:

> *"Our review suggests that the information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders."*[883]

106. Both panels' findings refuted Keith Alexander and President Obama's claims that "at least fifty threats" had been averted and "lives have been saved" as a result of bulk metadata retention. Both panels advised that the bulk surveillance program should be shut down. Section 215 was allowed to expire in May 2015.[884] The USA Freedom Act followed, reducing the capacity of the NSA to undertake mass collection of Americans' phone records, requiring instead that a subset of data be requested pursuant to limits set out in the Act.[885]

107. A number of former US intelligence professionals have publicly disclosed "bulk data failures" or blown the whistle on mass surveillance practices. William Binney, former Technical Director of the NSA has spoken out about the risk of "bulk data failure" since retiring after the September 11th 2001 attacks when much of the technology he had designed was subverted for mass surveillance. Binney has submitted evidence to the Joint Committee on the Draft Bill in which he described the bulk proposals as "*flawed and likely seriously to fail to serve current intelligence and data analysis problems for such purposes as Counter Terrorism"*[886]*.* Binney warned that, "*bulk data over collection*

---

[882] *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* – Privacy and Civil Liberties Oversight Board, 23 Jan 2014, p.11

[883] *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies* – 12 Dec 2013, p. 104

[884] *Section 215 Expires – For Now* – Mark Jaycox & Dia Kayyali, EFF, 31 May 2015

[885] USA Freedom Act 2015, available at: http://judiciary.house.gov/_cache/files/1cb59778-0a72-4c09-920d-0e22bf692bb4/fisa-01-xml.pdf.

[886] *Written evidence* – William Binney, 9 Dec 2015, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/25753.html

from Internet and telephony networks undermines security and has consistently resulted in loss of life in my country and elsewhere, from the 9/11 attacks to date". Instead, Binney advocates filtering at the point of collection, as he designed his original NSA program, rather than bulk collection and retention. In his evidence, Binney explains that such an approach would protect innocent citizens' privacy, protect privileged communications and relieve analysts of the burden of bulk data. Thomas Drake, a former senior executive at the NSA alongside Binney and later a whistle-blower, has also warned of the dangers of mass surveillance programs, both to civil liberties and national security. He has testified[887] that with a "smaller haystack" of data, the 9/11 attacks would have been preventable.[888] FBI whistleblower Coleen Rowley has also warned against mass surveillance systems following the 9/11 intelligence failures she experienced:

> *"I fear that terrorists will succeed in carrying out future attacks – not despite the massive collect-it-all, dragnet approach to intelligence implemented since 9/11, but because of it. This approach has made terrorist activity more difficult to spot and prevent."*[889]

108. Prior to the Snowden revelations, and in the wake of the murder of Fusilier Lee Rigby, former head of MI5 Dame Stella Rimington warned of the "well-known problem" of big data, drawing comparisons with the East German Stasi's "overdose" of information:

> *"Intelligence services can strangle themselves if they have too much information, because they can't sort out from it what they need to know and what they don't need to know."*[890]

109. Furthermore, scientists have rightly condemned *"how little of the debate [on mass surveillance] has dealt with the likely success of these tactics (…)",* arguing that *"the efficacy of such surveillance programs must be clearly understood if a rational policy is to be developed"*. The statistics journal *Chance* published a paper on the risk of automatic screening processes (such as those used for bulk interception, bulk data retention and upstream collection), which concluded that whilst a 99% accurate system would indeed report on 99% of the terrorists, the margin of error would also be responsible for producing hundreds of thousands, if not millions, of reports on innocent citizens.[891] This is partly the cause of "bulk data failure" that former intelligence professionals have described.

---

[887] Drake's testimonies to two Congressional investigations about 9/11 remain classified

[888] *After Paris, be careful what you ask for: an interview with Thomas Drake* – Thomas Drake & Mary Fitzgerald, 24 Nov 2015

[889] *The bigger the haystack, the harder the terrorist is to find* – Coleen Rowley, The Guardian, 28 Nov 2014, http://www.theguardian.com/commentisfree/2014/nov/28/bigger-haystack-harder-terrorist-communication-future-attacks

[890] *Terror watch lists: Can you keep tabs on every suspect?* – Ruth Alexander, BBC Magazine, 2 June 2013

[891] *Until proven guilty: False positives and the war on terror* – Howard Wainer & Sam Savage, Chance, March 2008, 21(1), pp.59-62, https://www.researchgate.net/publication/242713602_Until_proven_guilty_False_positives_and_the_war_on_terror

110. In every major terror attack in the Europe and USA since (and including) the 9/11 attack, including the Madrid bombings in 2004, the London 7/7 bombings in 2005, the murder of Lee Rigby in 2013, the Boston bombings in 2013, the January attack on the Charlie Hebdo offices and the Paris attacks in November 2015, some or all of the culprits have been known to the intelligence agencies. The failure to prioritise or action intelligence appropriately is commonly attributed to both human error and pressured resources – these reasons featured in the reports on the London 7/7 bombings[892] and the murder of Lee Rigby.[893]

111. No evidence has thus far been provided to illustrate a unique or critical contribution of bulk powers in combatting serious crime or indeed terrorism. Whilst in some cases bulk powers may offer helpful contributions to intelligence gathering, they have not (as far as is publicly known) proved critical in saving lives nor unique in providing intelligence that can be acquired through targeted methods. Furthermore, bulk powers clearly risk burdening intelligence agencies, whose incredible resources may be more effectively directed in targeted surveillance operations.

Is bulk surveillance proportionate?

112. It will never be proportionate in a democratic society during peacetime, to mass collect, monitor or process innocent communications in order to find those that threaten our security. Indeed this is why Britain – as opposed to totalitarian countries - has traditionally rejected this model. To take an example, the British postal service has never been required to intercept or store every letter or parcel it handles nor to make a note of the sender addressee and the time it was posted just in case the content or record of the package may in future be useful to the police or the security services. This important principle remains regardless of the mode of communication. Just because new ways of communicating electronically have made surveillance of innocents less expensive and burdensome than it may have been in the past, does not mean it is in society's interest to allow it.

113. The Government has previously attempted to argue that bulk interception is not intrusive if it is carried out by machines rather than humans. This is analysis is deeply flawed. There is nothing passive about mechanical State interception of communications and acquisition of communications data. The State cannot physically intercept a communication in a way that doesn't interfere with privacy just because it claims that human eyes will not necessarily see it.

114. Bulk surveillance also removes the possibility of safeguarding confidential and privileged communications. As a result of proceedings brought by Liberty and others, the IPT disclosed in June 2015 that **GCHQ had unlawfully intercepted and examined** private communications of **the Egyptian Initiative for Personal Rights (EIPR) and Legal Resources Centre (LRC) in South Africa**.[894] It later amended its ruling to clarify that the Agency had unlawfully intercepted and **examined Amnesty International's**

[892] *Could 7/7 Have Been Prevented? Review of the Intelligence on the London Terrorist Attacks on 7 July 2005* – Intelligence and Security Committee, 8 July 2008
[893] *Report on the intelligence relating to the murder of Fusilier Lee Rigby* – Intelligence and Security Committee, 25 Nov 2014
[894] The Tribunal did not make determinations concerning whether the other eight organisations had been intercepted.

communications rather than those of EIPR. GCHQ's activity was however only deemed unlawful because the Agency had breached its own internal guidance in a technical manner. The judgment provided no explanation as to why human rights NGOs had been bulk intercepted and individually examined and perversely did not find this action to amount to a breach of the ECHR. Indeed on its face the Draft Bill would permit the routine bulk interception and examination of human rights NGOs, lawyers, journalists, elected representatives and others.

115. Mass surveillance has significant and untested implications for the future of our society. David Anderson's report noted:

> *"the collection of vast volumes of data enables the identification of patterns and predictions of future behaviour, a process called predictive analytics, data mining or Big Data. An example of this technique is a predictive policing system called PredPol, which analyses large volumes of crime reports to identify areas with high probabilities for certain types of crime. The system has been used by Kent Police to predict when and where drugs crimes and robberies are likely to take place. PredPol is simply about when and where a crime will take place; other technology is aimed at predicting who will commit them. In 2011, the US Department of Homeland Security tested Future Attribute Screening Technology, which seeks to identify potential criminals by monitoring individuals' vital signs, such as cardiovascular signals and respiratory measurements. "* [895]

116. Liberty is concerned that the Agencies and law enforcement will in future seek to exploit so-called Big Data to predict behaviour. This would be a chilling shift in the relationship between the individual and State and could prove disastrous for the life chances of young people belonging to 'suspect' marginalised or disenfranchised groups.

117. The digital and technological revolution of the past fifteen years has led the Agencies to seek to collect ever-increasing troves of data and to devise mechanical programs to search databases for so-called suspicious patterns. Coupled with this, the current oversight model contains no checks on the Agencies overarching strategy which is instead self-determined and evaluated. However the current direction is unsustainable. Data is increasing exponentially. Liberty understands the agencies now have the capacity to hoover up 15 times the amount of data being collected when Edward Snowden blew the whistle in 2013. We urge independent parliamentarians and policy makers to reflect on the broader strategy and assess the value of harvesting overwhelming amounts of information.

Confidential and privileged correspondence

118. Liberty believes that the authorisation process for all types of surveillance in the Draft Bill falls short of that which is required by human rights standards. We are additionally alarmed by the complete absence of safeguards for the protection of confidential and privileged communications on the face of the Draft Bill.

MPs, Peers, MSPs, AMs, MLAs, MEPs

[895] David Anderson QC, A Question of Trust, paragraph 4.40

119. The communications data of MPs, Peers and other elected representatives receives no explicit protection in the Draft Bill. Data will remain accessible to a multitude of public authorities through the general system of self-authorisation.[896] MPs communications and devices will also be subject to mass interception, hacking and communications data acquisition by the Agencies under Part 6 of the Bill and MPs personal data will be acquired in bulk by them under Part 7. The only 'safeguard' against targeted hacking and interception is a requirement that the Secretary of State will 'consult' the Prime Minister before such targeted warrants are authorised.[897]

120. Until October 2015, it was widely understood that the communications of MPs were protected from interception by the Wilson Doctrine. On the 17th November 1966 the then Prime Minister, Mr Harold Wilson, said in a statement in the House of Commons:

> *"As Mr Macmillan once said, there can only be complete security with a police state, and perhaps not even then, and there is always a difficult balance between the requirements of democracy in a free society and the requirements of security. With my right hon. Friends, I reviewed the practice when we came to office and decided – on balance – and the arguments were very fine – that the balance should be tipped the other way and that I should give this instruction that there was to be no tapping of telephones of Members of Parliament. That was our decision and that is our policy. But if there was any development of a kind which required a change in the general policy, I would, at such moment as seemed compatible with the security of the country, on my own initiative make a statement in the House about it. I am aware of all the considerations which I had to take into account and I felt that it was right to lay down the policy of no tapping of telephones of Members of Parliament."*[898]

This protection, extended to members of the House of Lords in 1966, was repeated in unequivocal terms by successive Prime Ministers. Tony Blair clarified in 1997 that the policy *"applies in relation to telephone interception and to the use of electronic surveillance by any of the three Security and Intelligence Agencies."*[899]

121. Despite this clear and unambiguous statement that MPs and Peers would not be placed under electronic surveillance, in a recent decision the Investigatory Powers Tribunal held that the doctrine had been unilaterally rescinded by the Executive.[900]

---

[896] This follows the Government's statement March 2014 that it does not consider the Wilson doctrine to apply to communications data (HC Deb, 12 March 2014, column 306).

[897] Clause 16 and clause 85.

[898] HC Deb 17 November 1966 Vol 736, columns 634-641.

[899] HC Deb 4 December 1997 Vol 302, Col 321.

[900] In October 2015, the IPT held that the Wilson Doctrine was not absolute and in any case not legally binding and that the protection of politicians' correspondence was instead regulated by secret security service Internal Guidance which was only disclosed over the course of the litigation. Under this Guidance, targeting of a politician will be "exceptional" but not prohibited, and politicians may have their communications gathered by mass interception powers. Where targeted interception takes place, the usual process of political warrantry will apply with "particularly careful consideration" given to the necessity and proportionality of surveillance. A number of individuals within the relevant agency must be informed and their advice invited, which must be recorded on the Central Record. The DG must be consulted before the application is made to the Secretary of State and before deciding on a warrant. Before deciding whether to issue a warrant *"the Secretary of State will need to consult the Prime Minister via the Cabinet Secretary".* This process is now referenced in the Draft Bill.

Liberty disputes this finding. The unequivocal statement made by Prime Minister Wilson back in 1966 was a constitutional convention protecting vital discourse between the people and their ultimate representatives, creating a legitimate expectation on the part of parliamentarians and their constituents that their correspondence was protected. However, there is currently no right of appeal against decisions of the IPT.

122. Liberty believes it is illogical to suggest that an adequate replacement to the previous complete prohibition on surveillance of politicians is to require the Secretary of State to consult with the Prime Minister prior to signing a targeted interception or examination warrant. Instead of securing an independent system, involving two politicians rather than one makes the process more political rather than less. It is difficult to see why Members of Parliament and other elected representatives should have confidence that "consultation" with the Prime Minister can act as a bulwark against unjustified surveillance. Liberty does not suggest that parliamentarians should be above the law, but in recognition of their unique constitutional role we advocate a strong legislative presumption against surveillance of elected representatives, that can only be rebutted in in clear and specific circumstances overseen by judicial commissioners.

Journalists

123. Clause 61 would require a public authority to apply to a Judicial Commissioner to confirm an authorisation to obtain communications data for the purpose of identifying or confirming journalistic sources. A Judicial Commissioner may approve the authorisation if the requirements of Part 3 are met. The Bill is silent on protections against the interception or hacking of journalists.

124. In September 2014 it was revealed that the Metropolitan Police had used the RIPA internal authorisation route to access communications data of a journalist from The Sun newspaper as part of their "plebgate" inquiry, circumventing the well-established judicial process set out in the Police and Criminal Evidence Act 1984. In response to public outcry, the Government updated the Acquisition and Disclosure of Communications Data Code of Practice, advising law enforcement that where an application to access the communications data of a journalist in order to determine the source of journalistic information is made, it must be via the PACE route. PACE sets out the special procedures that must be followed if law enforcement agencies wish to access material that may be journalistic or confidential journalistic material. To access journalistic material, which comes under the broad definition of *"material acquired or created for the purpose of journalism",* an application must be made to a judge. The conditions that must be met before the judge can grant a warrant include: there are reasonable grounds for believing an indictable offence has been committed; the material is likely to be of substantial value; and, other methods of obtaining the material have been tried or are bound to fail. In addition to these requirements, the judge must be convinced that it is in the public interest to grant access to the materials. In order to access confidential journalistic material – namely information relating to sources – PACE sets out that a warrant will only be granted if prior to PACE it would have been possible to access source material via a power contained in primary legislation. As a result, it is only in very rare circumstances

that an order will be made under PACE to reveal confidential journalistic material. Unlike the process contained in the Draft Bill, both these processes are *inter-partes*, giving the journalist the opportunity to make their case to the judge. It is also possible to gain access to confidential journalistic material under the Terrorism Act 2000.

125. The mechanism introduced by clause 61 is inadequate to secure the independence and vitality of our free press. It allows for a circumvention of the established and much more rigorous PACE process, creating a system in which communications data can be accessed without the PACE protections.

126. Liberty believes that the PACE protections should be restored for access to journalistic communications data and that equivalent protections should be in place to safeguard against the equally if not more intrusive hacking powers contained in the Draft Bill.

Lawyers

127. Legal privilege is an essential protection in a free society governed by the Rule of Law. The doctrine is intended to ensure fair trial integrity and ensure both defendants and civil claimants can communicate with their lawyers without inhibition. Legally privileged communications are those between a client and their lawyer which come into existence for the dominant purpose of being used for legal advice or in connection with actual or pending litigation. Legal privilege does not apply where client-lawyer communications are made in furtherance of a criminal activity.

128. Legal privilege has traditionally been protected at common law and under Article 6 HRA. Like the Wilson Doctrine it was considered absolute. However, public interest litigation brought over the course of 2014-15 has revealed a set of internal Government policies that render LPP illusory.

129. Abdel Hakim Belhaj alleges he is a victim of CIA-SIS rendition and torture and is attempting to hold the UK Government to account for this. During the course of legal proceedings and in the wake of the Snowden revelations, his lawyers came to fear that they were under surveillance. In the course of proceedings before the Investigatory Powers Tribunal the Government conceded that **"since January 2010 the policies and procedures for the interception/obtaining, analysis, use, disclosure and destruction of legally privileged material have not been in accordance with human rights legislation specifically Article 8(2) of the ECHR."**[901] Instead, they allowed for legally privileged communications of between a victim of SIS-CIA rendition and torture and his lawyer to be targeted for surveillance. It is unacceptable that the Government could have used its surveillance powers to undermine attempts to hold it to account for its complicity in torture, but that is what existing legislation has permitted and this would remain permitted under the terms of the Draft Bill.

[901] "Government concedes policies on lawyer-client snooping were unlawful", Reprieve, 15 February 2015, available at - http://www.reprieve.org.uk/press/government-concedes-policeson-lawyer-client-snooping-were-unlawful/

130. The Draft Bill therefore represents an important and timely opportunity to ensure statutory protection for LPP. However, as weak as the protections in the draft Bill are for politicians and journalists, LPP – along with the communications of other professions who handle confidential material such as medical doctors and NGOs - is not even granted the dignity of a name check. The Government intends that the only protection to be offered to these communications will come via a Code of Practice, likely to mirror the weak and ineffective Codes of Practice that already govern this area.[902] This is a wholly unacceptable position which risks fatally and fundamentally undermining fair trial rights in the UK.

Recommendations

- For as long as mass surveillance powers prevail, there is no way to ensure that confidential and privileged communications content and records will not be intercepted, hacked and transferred in bulk to the Agencies with the rest of our communications. To that end the Draft Bill proposes to enshrine in law for the first time, the power to subject MPs, journalists' and lawyers' communications to bulk surveillance practices. As we argue at paragraphs 80-116) Liberty strongly advocates an end to undemocratic mass surveillance.
- **In addition to ending mass surveillance practices, Liberty believes there should be an extremely strong legislative presumption against the targeted interception, hacking, and acquisition of communications data and all other forms of targeted surveillance against elected representatives, journalists and lawyers. The conditions that must be met before a judicial commissioner can grant a surveillance warrant targeting a member of these groups should mirror the current regime for production orders of journalistic material under PACE, namely (a) there are reasonable grounds for believing an indictable offence has been committed, (b) the material is likely to be of substantial value, (c) other methods of obtaining the material have been tried or are bound to fail. In addition to these requirements, the judge must be convinced that it is in the public interest to grant access to the materials.**

Encryption

131. Computer security, like all data security, centres on the aim of protecting information from unauthorised access. Encryption is the leading tool in computer security. Encryption is a method of protecting communications or data from unauthorised access and is widely used to protect online browsing, credit card details, online retail, emailing and messaging, medical data, transport infrastructures, proprietary business information, and much more. 'Third party encryption' is that which is supplied by a communications service (such as Google, Facebook), and which is most affected by this Draft Bill. Greater security is found in client-side encryption, whereby the user encrypts information using keys they have generated and that only they (not their service provider) possess. This

[902] See for example, the revised Interception Code of Practice, published in 2015. Liberty's response to the consultation on the Draft Code is available at - https://www.liberty-human-rights.org.uk/sites/default/files/Liberty's%20response%20to%20the%20Home%20Office%20consultation%20on%20the%20Interception%20of%20Communications%20Code%20of%20Practice%20(Mar%202015).pdf.

personally managed encryption features in popular free software such as TrueCrypt (file encryption) and PGP (email encryption).

132. Despite the Home Office's claim that the draft Investigatory Powers Bill "*will not impose any additional requirements in relation to encryption over and above the existing obligations in RIPA"*[903]*,* it presents a renewed and expanded assault on encryption that will dramatically diminish privacy and security online. Although it is situated rather modestly in the draft Bill, clause 189 in Part 9 contains the significant power for a Secretary of State to oblige telecommunications operators, both domestic and overseas, to covertly remove encryption from their services, thus enabling the Government to intercept any communications or data.[904]

133. The State already has several means to circumvent encryption. Under Section 49 of RIPA 2000, a person using encryption can be compelled to decrypt any information, thus providing it in plaintext, intelligible form; or to hand over the relevant encryption key. Notices can also be issued to attain any information which would facilitate the obtaining or discovery of a key. Police and intelligence agencies also currently claim the power to hack devices, thus circumventing encryption, under the Police Act 1997 and the Intelligence Services Act 1994 respectively. This power is restated and broadened in Part 5 of the draft Bill, with further provisions to perform mass hacking without suspicion in Part 6 (Chapter 3).

134. Despite these powers to require decryption and circumvent encryption via hacking, the Draft Bill proposes to renew the power to force "*the removal of electronic protection"* from communications services, and expand capabilities to remove encryption by broadening the framing of the power. RIPA 2000 and paragraph 10 of the Schedule to *the RIPA (Maintenance of Interception Capability) Order 2002*[905] grants the State the power to force "*public telecommunications services"* to remove encryption. Under the Draft Bill communications services can be imposed with obligations not only to remove "*electronic protection"*, but with additional obligations including those "*relating to the security"* of the service provided, relating to "*apparatus owned or operated"* by the service, and "*obligations to provide facilities or services of a specified description" – "among other things"*[906]*,* which remain undefined. Whereas provisions under RIPA oblige "*public telecommunications services"*[907] [908] to remove encryption, the draft Bill would oblige any "*telecommunications services"*[909], which are defined as *"any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service)"*[910]. This expanded definition would include not only public services such as

[903] *Draft Investigatory Powers Bill 2015: Guide to Powers and Safeguards,* p.29
[904] *Draft Investigatory Powers Bill 2015,* clause 189, subsection (4)
[905] *Regulation of Investigatory Powers Act 2000,* section 12 (1);
[906] *Draft Investigatory Powers Bill 2015,* clause 189, subsection (4).
[907] *Regulation of Investigatory Powers Act 2000,* section 12 (1).
[908] *The Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002,* section 10.
[909] *Draft Investigatory Powers Bill 2015,* clause 189, subsection (2)(b).
[910] *Draft Investigatory Powers Bill 2015,* clause 193, subsection (11).

Gmail, Facebook, Twitter and Dropbox, but also private offices, businesses, law firms, government department networks (such as the NHS), and institutional networks such as universities. Obligations to remove electronic protection can be issued in either a 'national security notice' or more likely, a 'technical capability notice' from the Secretary of State.[911] There is no judicial authorisation required for either notice. The recipient of such a notice must comply with it[912] but must not disclose the existence or contents of it.[913]

135. Encryption is now a widely used standard to protect the ever-expanding uses of communications technologies in an increasingly hostile digital environment: from mobile phones and smart phones to personal hard drives, online banking and e-commerce, critical infrastructures, transport networks, institutional and business computer networks, cloud storage, emailing and messaging, web browsing and online shopping. The renewed and extended assault on encryption in the Draft Bill demonstrates a misguided commitment on the part of the State to undermine secure spaces in the furtherance of mass surveillance ambitions.

136. These powers do not require prior judicial authorisation or a test of necessity and proportionality. This means that the specific risks and technical consequences that removal of electronic protections and other measures to maintain interception capabilities may incur are not considered when warrants are issued under other Parts of the Bill. It is also concerning that obligations under clause 189 may not necessarily relate to an existing warrant or authorisation. Therefore, a service provider could be compelled with obligations to remove encryption and security measures, perhaps with a view to seeking a warrant for interception in the future, but not necessarily currently holding that warrant. This means that the obligations could be served without even an indirect consideration of necessity and proportionality. It also means that the unprotected material would be easier for any actor to intercept with or without a warrant.

137. Encryption is a critical tool for protecting individuals' rights to privacy and freedom of expression – particularly for those in sensitive professions, and discriminated and minority groups. In a 2015 report, David Kaye, the United Nations Special Rapporteur on Freedom of Expression, described encryption as a leading vehicle for online security and freedom, giving individuals:

> *"a means to protect their privacy, empowering them to browse, read, develop and share opinions and information without interference and enabling journalists, civil society organisations, members of ethnic or religious groups, those persecuted because of their sexual orientation or gender identity, activists, scholars, artists and others to exercise the rights to freedom of opinion and expression."*[914]

---

[911] *Draft Investigatory Powers Bill 2015,* clause 190, subsection (1)
[912] *Draft Investigatory Powers Bill 2015,* clause 190, subsection (9)
[913] *Draft Investigatory Powers Bill 2015,* clause 190, subsection (8)
[914] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye* – UN Human Rights Council, 22 May 2015, paragraph 1

138. In addition to protecting freedom of expression, Kaye found encryption "*essential"* for the exercise of further vital rights, including "*economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity"*[915]*.* Kaye analysed submissions on the laws and policies of member states as well as submissions from civil society groups, leading him to conclude:

> *"States should not restrict encryption (…) which facilitate(s) and often enable(s) the rights to freedom of opinion and expression* (…) *States should avoid all measures that weaken the security that individuals may enjoy online, such as backdoors, weak encryption standards and key escrows"*[916]

139. Undermining encryption seriously jeopardises the security of technologies, their users, and modern digital society as a whole. David Anderson found:

> *"Few now contend for a master key to all communications held by the state, for a requirement to hold data locally in unencrypted form, or for a guaranteed facility to insert back doors into any telecommunications system. Such tools threaten the integrity of our communications and of the internet itself."* [917]

However, these practices would indeed be the consequence of clause 189 in the draft Bill. The Information Technology Industry Council (ITI), which represents 62 of the largest technology companies worldwide including Apple, Microsoft, Google, Samsung, Twitter, and Facebook released a statement following the publication of the draft Bill in defence of encryption:

> *Encryption is a security tool we rely on every day to stop criminals from draining our bank accounts, to shield our cars and airplanes from being taken over by malicious hacks, and to otherwise preserve our security and safety. We deeply appreciate law enforcement's and the national security community's work to protect us, but weakening encryption or creating backdoors to encrypted devices and data for use by the good guys would actually create vulnerabilities to be exploited by the bad guys, which would almost certainly cause serious physical and financial harm across our society and our economy.*[918]

140. In a recent research paper by world leading technologists, it was concluded that US and UK governments' proposals to achieve "exceptional access" to encrypted communications would "*raise enormous legal and ethical questions, and would undo progress on security at a time when Internet vulnerabilities are causing extreme economic harm"*[919]. Security experts agree. In a recent op-ed for the Washington Post

---

[915] Ibid, paragraph 56

[916] Ibid, paragraph 60. Note: a key escrow is an arrangement in which cryptographic keys are entrusted to a third party (in this context, the state).

[917] *A Question of Trust: Report of the Investigatory Powers Review* – David Anderson Q.C., June 2015, paragraph 13.12, p.248

[918] *Tech Responds to Calls to Weaken Encryption* – Information Technology Council, 19 Nov 2015

[919] *Keys Under Doormats* – H. Abelson, R. Anderson, S. M. Bellovin, et al., MIT, 7 July 2015

Mike McConnell, the former Director of the NSA, Michael Chertoff, former Secretary of Homeland Security and William Lynn, the former Deputy Secretary of Defence argued that, in order to protect economic and national security, encryption should not be undermined for Government surveillance. They concluded, "*(w)e believe that the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server and enterprise level without building in means for government monitoring*"[920].

141. There is increasing awareness in the US of the dangers of undermining encryption for mass surveillance purposes. A recent draft opinion paper on strategic approaches to encryption from the National Security Council argued that "*(o)verall, the benefits to privacy, civil liberties and cybersecurity gained from encryption outweigh the broader risks that would have been created by weakening encryption*". The NSC concluded, "*the Administration will not seek legislation that compels providers to enable government access to encrypted information, even pursuant to lawful process*"[921]. Apple's Chief Executive Tim Cook has argued against government attempts to 'backdoor' (i.e. seek or create vulnerabilities in software to achieve unauthorised access) encryption, explaining, *"(t)o protect people who use any products, you have to encrypt (…) Any backdoor is a backdoor for everyone (…) Opening a backdoor can have very dire consequences*"[922]. The UK's national cybersecurity, is an increasingly critical element of our national security. As stated by the Information Technology Council, "*weakening security with the aim of advancing security simply does not make sense"*[923].

142. In addition, the Software and Information Industry Association (SIIA) submitted written evidence to the Science and Technology Select Committee regarding the Draft Bill, seeking clarification on provisions relating to encryption, and expressing concerns about the pressure to respond to similar requests from multiple governments:

> *Should Western democracies require "backdoors," companies will not have a credible reason not to provide backdoors to other countries. This increases the exposure of critical infrastructure and individuals to attacks and spying from nation state actors, as well as from terrorists and criminals.* [924]

143. The free software community Mozilla, whose web browser 'Firefox' encrypts 100 billion individual web data transfers every day, also submitted written evidence expressing the same concern.[925]

---

[920] *Why the fear over ubiquitous data encryption is overblown* – Mike McConnell, Michael Chertoff & William Lynn, The Washington Post, 28 July 2015

[921] *Review of Strategic Approaches* – National Security Council; cited in *Obama faces growing momentum to support widespread encryption* - Ellen Nakashima & Andrea Peterson, The Washington Post, 16 Sept 2015

[922] *Apple's Tim Cook declares the end of the PC and hints at new medical product* – Allister Heath, The Telegraph, 10 Nov 2015

[923] *Tech Responds to Calls to Weaken Encryption* – Information Technology Council, 19 Nov 2015

[924] *Written evidence regarding Investigatory Powers Bill* - Software & Information Industry Association, 1 Dec 2015

[925] *Written evidence regarding Investigatory Powers Bill* - Mozilla, 1 Dec 2015

144. "*The voice of the internet industry"*, the Internet Service Providers Association (ISPA) has expressed concern that "*attempts to undermine encryption could damage user trust in online services*".[926] Indeed, if the provision to force removal of encryption is passed it is very likely that users – particularly those in sensitive sectors such as law, journalism and health - will move away from UK technologies and towards providers based in countries that do not undermine security, thus damaging the UK's digital economy. Furthermore, some UK providers may have to discontinue services if they do not wish to mislead customers as to the security features, or indeed if their product design does not include a mechanism by which to remove users' encryption.

145. Anyone intent on evading surveillance need not rely on a telecommunications service to provide encryption, but can easily use open source encryption software with personally generated and managed keys. This type of client-side encryption, typically used to encrypt files and email communications, is independent of third party providers, and as such would remain unaffected by this legislation. The proposal to force telecommunications services to allow government access to masses of encrypted communications, by an offline analogy, is akin to forcing every locksmith to retain duplicates or a master key to thousands of houses to enable suspicionless property searches. By any usual test, this would not be considered a necessary or proportionate measure.

Recommendations

- Liberty believes the power to remove or in any way undermine encryption over entire communication services indiscriminately denies millions of people the right to privacy, and jeopardises freedom of expression. Therefore, Liberty believes that the requirement to remove encryption should be removed from clause 189.
- We concur with David Anderson's view that *"(f)ar preferable, on any view, is a law-based system in which encryption keys are handed over (by service providers* [if they have them] *or by the users themselves) only after properly authorised requests*".[927] This should be a tightly regulated power subject to judicial authorisation, and exercised only in the interests of investigating serious crimes. Anderson argued that the best way to set an example to other nations, thus protecting international cybersecurity, is "*by demonstrating an ability to patrol those spaces in tightly defined circumstances, and with sufficient safeguards against abuse*".[928]

Intelligence Sharing

146. Liberty is disappointed that the Bill is silent on the intelligence sharing relationship between the Agencies and foreign intelligence agencies, in particular the Five Eyes. The Reviewer's report described an "international trade in intelligence" between the Five Eyes partners – the UK, USA, Canada, Australia and New Zealand. Insofar as material gathered by the British services is shared with other countries, the report explains that

[926] *Internet industry has major concerns on the Investigatory Powers Bill,* ISPA Conference press release, 19 Nov 2015
[927] *A Question of Trust: Report of the Investigatory Powers Review* – David Anderson Q.C., June 2015, paragraph 13.12, p.248
[928] Ibid. Paragraph 13.14, p.248

the security services take the view that under their founding statutes, information can be shared if it is *"necessary for the purpose of the proper discharge of the security and intelligence agencies' functions"* and that when it is considered that this test is met certain RIPA safeguards apply. However, the report concludes that *"in practical terms, the safeguards applying to the use of such data are entirely subject to the discretion of the Secretary of State."*[929] The report also states that RIPA imposes no limits on the sharing of communications data obtained from service providers with overseas governments, although the Acquisition Code provides some guidance for dealing with requests for information.[930]

147. RIPA and the Codes of Practices are silent on British services receiving or accessing information from foreign services, with the security services only limited by the "general constraints" on their actions in various statutes.[931] It was only during the course of Liberty's legal action against the security services in the IPT that limitation information about the way in which the security services approach such situations was revealed. In its first finding against the Agencies, the IPT held that prior to these disclosures, the framework for information sharing was not sufficiently foreseeable and was not therefore "in accordance with law". The Tribunal held that as a result of the fact that the litigation had resulted in disclosures of information, the security services were no longer acting unlawfully when accessing information from the U.S..

148. David Anderson's report recommends that information sharing with foreign countries be subject to strict, clearly defined and published safeguards.[932] The report adds that the *"the new law should make it clear that neither receipt nor transfer as referred to in recommendations 76-77 above should ever be permitted or practised for the purpose of circumventing safeguards on the use of such material in the UK".*[933] Such safeguards and guarantees are notably absent from the Draft Bill.

Oversight

149. The Draft Bill proposes that the Investigatory Powers Commission (IPC) will replace the Interception of Communications Commissioner Office (IOCCO), the Office of Surveillance Commissioners (OSC) and the Intelligence Services Commissioner (ISCom). Their roles will be divested in the newly created Investigatory Powers Commissioner and fellow Judicial Commissioners who will therefore have dual responsibility (a) for reviewing Secretary of State and chief constable surveillance warrants and (b) for oversight of the use of intrusive powers. The IPC is additionally required to keep under review any aspect of the functions of the Agencies as directed by the PM[934] and these directions need not be published if PM considers it would be contrary to the public

[929] Paragraph 6.87.
[930] Paragraph 6.88.
[931] Paragraph 6.89.
[932] Recommendations 76 and 77.
[933] Recommendation 78.
[934] Draft Investigatory Powers Bill, Clause 170.

interest or prejudicial to the three grounds or the continued discharge of the functions of any public authority whose powers are reviewed by the IPC. The IPC must make an annual report to the PM about the carrying out of the functions of the JCs

150. Liberty supports the creation of a single body to undertake the duties and functions currently covered by a range of different surveillance commissioners. This confuses the roles of authorisation and oversight. It is constitutionally inappropriate for those involved in the decision-making process to also bear responsibility for oversight of those decisions. The conflation of these responsibilities gives rise to a conflict of interest. This is demonstrated by clause 169 which imposes obligations on Commissioners not to act in a way that may inhibit the effectiveness of particular operations when undertaking oversight functions. JCs are then told to disregard these obligations in circumstances where the JC is involved in reviewing warrants.

Recommendation

- Liberty supports the consolidation of the byzantine model of surveillance oversight currently provided by several commissioners. However we are deeply concerned the Draft Bill hands these functions to the newly created body of JCs. **JCs independence and perceived independence will be wholly undermined by the clear conflicts of interest that will likely arise on a regular basis.** We believe that oversight of intrusive powers should be vested and consolidated in a new body independent from the IPC, IPT and Executive.

Post surveillance notification

151. Liberty believes that JCs should be under a mandatory statutory duty to notify those subjected to surveillance once a particular operation or investigation has ended. At present unlawful surveillance only comes to light as a result of a chance leak, whistleblowing or public interest litigation brought by Liberty and other NGOs and concerned citizens. This is deeply unsatisfactory.

152. If a person's Article 8 and other HRA protected rights have been infringed, in order to have access to an effective remedy as required under human rights law, the person must first be made aware of a possible breach. This was stated by the ECtHR in *Klass v Germany* in 1978 and reiterated in *Weber and Saravia v Germany* in 2006:

> *"The Court reiterates that the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively"* (see Klass and Others, cited above, pp. 26-27, § 57).[935]

153. In *Zakharov v Russia* the ECtHR found that that judicial remedies for those subjected to interception in Russia were generally ineffective, particularly in light of the total

[935] Weber and Saravia v Germany, 2006, application 54934/2000, paragraph 135.

absence of any notification requirement with regard to the interception subject, without any meaningful ability of retrospective challenges to surveillance measures.

154. The Draft Bill provides a new power for the JCs to inform someone subjected to a surveillance error if the JC is made is aware of it; considers it sufficiently serious and the IPT agrees that it is a serious error and that it is in the public interest for the person concerned to be informed.[936] For it to be serious it must have caused '*significant prejudice or harm to the person concerned*'. The Draft Bill states that a breach of the HRA is not sufficient for an error to be considered a serious error. Before making its decision the Tribunal must ask the public authority responsible for the error to make submissions to the Tribunal about the seriousness of the error and the public interest in disclosure. This is a narrow, arbitrary and highly discretionary power that will relate only to the most serious errors that the JCs discover during their very limited audit of the use of surveillance powers. It highlights the conflicted position that JC's may find themselves in and it does not discharge the Government's human rights obligations to provide post notification by default unless it can justify continued secrecy.

Recommendation

- **Liberty believes that in order to ensure accountability for surveillance, JCs should be required to notify those subjected to surveillance after an investigation or operation has ended unless there is an objectively justifiable reason for maintaining secrecy.**

Reform of the Investigatory Powers Tribunal

155. Liberty has long advocated reform of the Investigative Powers Tribunal, the secretive body which hears cases involving state surveillance. The Tribunal is not required to hold oral hearings; hearings do not need to be *inter-partes;* it cannot disclose the identity of a person who has given evidence at a hearing or the substance of the evidence unless the witness agrees. If the Tribunal finds against a complainant it cannot give its reasons for doing so, meaning that the individual does not know whether no surveillance took place or whether lawful surveillance took place, and if it upholds a complaint is it only required to provide the complainant with a summary of its reasoning. Its judgements are therefore opaque.

Recommendation

- As *Justice* noted in their 2011 report, half of the successful complainants to the IPT concerned cases where those concerned had been notified of surveillance. Of the three successful claims brought in 2015, the cases were brought only as a result of the Snowden disclosures. To this end, the most significant reform that could improve the effectiveness of the IPT would be a requirement for post notification of all targeted surveillance.

[936] The definition of an error includes failure to comply with requirements under this Act and in Code of Practice under Schedule 6.

- Liberty encourages parliamentarians to establish a principle of open proceedings in the IPT, with the option for the tribunal to determine that closed or partly closed hearings are in the interests of justice.

Appeals

156. Liberty welcomes the granting of a right of appeal from the IPT in the Draft Bill which inserts new clause 67A RIPA. This creates a right of appeal and specifies that the appeal only lies against the final determination of a claim / complaint and leave to appeal will only be granted if the appeal would raise an important point of principle or practice or there is another compelling reason for granting leave. Leave for an appeal can be granted by the Tribunal or the Court who would hear the appeal.

Recommendation

- Liberty believes that the right of appeal should be extended to cover any IPT ruling on a point of law, including in the *course* of proceedings, as was the case in Liberty's recent claim in the IPT.
- Liberty believes that the Draft Bill should specify which court the appeal would lie to, rather than the Court of Appeal in England and Wales and equivalent courts in Scotland and NI *unless the Secretary of State provides otherwise*. This is important for costs purposes as CPR 52.9A gives the Court of Appeal the power to limit costs liability when a case comes to it from a non-costs jurisdiction. This would not be the case if the appeal were to a different court.
- Liberty further advocates that the IPT should be given the power to make a declaration of incompatibility under the *Human Rights Act 1998* and notes that David Anderson supported this recommendation.

22 December 2015

LINX—written evidence (IPB0097)

Executive summary

1. We welcome the decision to introduce new legislation to replace Part 1 of the Regulation of Investigatory Powers Act 2000 and associated legislation. Such legislation was needlessly complex and unclear, and its impact in the context of the greatly increased use of Internet communications justifies Parliament's attention.
2. We also welcome a number of specific provisions in the Draft Bill in relation to oversight.
3. We also welcome the government's continuing commitment to the reimbursement of compliance costs, although we consider that this should appear in the Draft Bill as duty for the Secretary of State, rather than merely a power.
4. We do warn that rushing this legislation may result in a swift return to Parliament in the light of foreseeable European developments.
5. We do not support the assertion of extra-territorial authority in the imposition of requirements on telecommunications operators outside the UK. This is unfair to them, and sets a dreadful precedent for foreign governments that is likely to rebound to the harm of UK business in general, and UK Internet businesses in particular.
6. We believe that the Draft Bill imposes an excessive degree of secrecy concerning the use of its powers. While we accept the need for operational secrecy, the requirements as written will impair democratic scrutiny and the effectiveness of legal oversight.
7. We note that the Draft Bill includes changes to the law on interception designed to enable additional blocking or "censorship" of Internet content on a voluntary basis, without the need for further legislation. Our members' views on this vary.
8. We consider the powers for "national security notices" and "technical capability notices" to be far too broad. Parliament cannot know what it is authorising, nor can telecommunications operators know what to expect, except by closed door discussions with officials. This is not what the rule of law looks like.
9. We do not support requiring telecommunications operators to build "backdoor access" into what ought to be strong end-to-end encryption protecting customer communications. On balance, the security such encryption provides is very much to the benefit of the UK, and introducing deliberate vulnerabilities of this, or any other nature, would be most unwise.
10. We are concerned that the drafting of the definitions "relevant communications data" and "communications data" appear inconsistent with the Home Secretary's assurance that the Draft Bill is not intended to require ISPs to collect third party data. We would strongly object to such an imposition, and urge the definitions to be clarified to avoid any possibility that they could be so interpreted.
11. We also provide technical advice to the committee about the impact and meaning of key defined terms: "Internet Connection Records", "Entity Data" and "Location". We note that these will result in the Draft Bill being very much more intrusive in terms of privacy and confidentiality than RIPA has been, let alone what was envisaged when RIPA was enacted by Parliament. We do not offer a conclusion as to whether this is justified, but offer some detailed illustrations for the benefit of the Joint Committee.

12. We also provide, for the benefit of the Joint Committee, an explanation of the enormous technical power the "filtering arrangements" represent in terms of being able to analyse communications data, and provide illustrations of what could theoretically be done with it.
13. We set out our concerns that the powers in this Draft Bill rest far too heavily on the unsupported concept of "proportionality". We believe that this cannot be an adequate safeguard for such broadly defined powers, especially since there are no statutory standards, principles or guidance to assist those who use the powers in assessing what is proportionate.
14. In particular, we have serious concerns that the powers for "equipment interference" fail to protect against damage to critical infrastructure.

About LINX

15. LINX, the London Internet Exchange, is a membership association for network operators and service providers exchanging Internet traffic. It is part of our core mission to represent our members' interests in matters of public policy.

16. With more than 650 member organisations, including most major UK ISPs and most formerly-incumbent European operators, we believe we have highly informed expertise and are well placed to reflect the views of the ISP industry as a whole.

17. LINX has worked on behalf of its members on the development of policy for covert investigation of communications, including communications data since before the inception of the Regulation of Investigatory Powers Act 2000. We have worked in cooperation with the Home Office and law enforcement representatives to develop primary and secondary legislation, Codes of Practice, building a partnership between the ISP industry and law enforcement interests. A LINX employee also represented the European Internet industry on the European Commission's Experts' Group on the Data Retention Directive when that group (and Directive) was active.

18. We are committed to a regime for communications data retention and access that is both effective in meeting law enforcement needs and also respectful of the legitimate interests of the Internet industry, our members, and of the general public, the customers and end-users of our members.

19. We have consulted our membership both informally and formally, during the development of this policy over the past several years. We would never say that any submission by us is endorsed by every one of our members in every last detail, but we do believe that our position reflects a broad view in the network operator community.

General points of welcome

20. LINX welcomes that the government has decided to bring forward new legislation largely to replace Part 1 of the Regulation of Investigatory Powers Act 2000 (RIPA), as well as the Data Retention and Investigatory Powers Act 2014. This legislation is

notoriously complex and arcane, and certainly due for review in the light of changing technology, and the changing way the public use the services covered by these Acts.

21. We welcome the opportunity to clarify and consolidate the relevant legislation. We also welcome the opportunity to review it to ensure that it still meets the legitimate needs of the law enforcement and intelligence and security community, and the opportunity to subject it to renewed democratic scrutiny so that the impact of the legislation on the fundamental rights of individuals and businesses may be reconsidered. We also welcome the opportunity to consider the burden on the telecommunications operators who must comply with it.
22. We therefore also welcome the abolition of legacy powers[937], not only those in RIPA and associated legislation.
23. We would also like to welcome some of the specific measures the government proposed in the Draft Bill:
    a. We welcome the merger of the different RIPA Commissioners into an Investigatory Powers Commissioner. The separation was confusing the public, and created the potential for duplication. More importantly, it reduced transparency and undermined the ability of any of them to build public confidence in the investigatory powers regime.
    b. We also welcome the continued commitment to oversight by Single Points of Contact, which has been one of the more successful innovations introduced in the implementation of RIPA.
    c. We welcome the introduction of new offence that can be committed by misusing a position in a public authority to gain access to communications data unlawfully[938]. With extraordinary powers comes extraordinary responsibility, and it is important that those who betray that trust can be seen to be held accountable. The principle of criminal accountability for misuse of public powers is an important one, whose introduction we would welcome in other similar situations.
    d. We also welcome that the secrecy rules relating to interception have been adjusted to allow telecommunications operators to ask for, and receive, professional legal advice in relation to their obligations[939].

European legislation and legal challenges

24. We note that since the Court of Justice of the European Union quashed the EU Data Retention Directive in the case *Digital Rights Ireland*, European institutions have been considering bringing forward new measures in this area at the European level.
25. While we recognise the urgency of making replacement provision before the expiry of the sunset clause on DRIPA (2014), we are concerned that if we rush into substantial new legislation in the UK it may have barely reached the statute book before we are forced to consider supervening EU instruments.
26. We also note the ongoing case, *David, Watson et al v Secretary of State for the Home Department*. At first instance, this would have disapplied DRIPA from March 2016, and would have had a serious impact on the compatibility of many of the provisions

[937] See s(9).
[938] See s(8).
[939] See s43(5)(f)

of the Draft Bill with European law. That case has now been referred to the Court of Justice of the European Union, asking whether the CJEU intended in *Digital Rights Ireland* to set controlling standards for Member States.

27. Accordingly, we do not consider it will be possible to achieve confidence in a new settled regime in this area until these matters are resolved. That calls into question whether it is really appropriate to bring this Bill before Parliament until these issues are known. If the government were willing to wait, we believe a more thorough investigation by this Joint Committee than the current timetable permits would be enormously beneficial. We are aware that the government is currently stressing urgency, but the outcome in *Davis, Watson et al* and a new legislative initiative from the European Commission have the potential to change the government's mind.
28. If Parliamentary procedure permits, we would suggest to the Joint Committee that it might consider issuing its report as an Interim Report, and remain constituted to consider these matters in more detail over the coming months. Alternatively, we would invite the Joint Committee to consider the value further work by a Committee constituted like itself could bring, and to make appropriate recommendations in its report.

Cost reimbursement

29. We welcome that there is provision made in the Draft Bill for reimbursement of the costs telecommunications operator incur in complying with the measures in the Draft Bill.
30. The Draft Bill requires the Secretary of State to make a contribution to these costs, but does not specify what it might be, other than that it may not be nil.
31. The current government's policy, as it has been every government's policy since RIPA, is essentially to pay the full costs reasonably incurred, as assessed by the Secretary of State (without allowing for profit).
32. We believe that the Bill should require the Secretary of State all the costs that she assesses as having been reasonably incurred by the telecommunications operator in order to comply with obligations imposed on them under the Bill.

Assertion of extra-territorial authority

1. We note that the Draft Bill purports to impose obligations in Parts 2, 3 and 4 on telecommunications operators outside the UK.
2. We consider this to be wrong in principle and likely to cause great difficulties in practice.
3. The assertion of extra-territorial authority will rob the United Kingdom of a principled basis for dissuading or criticising foreign governments from following this precedent, and will indeed encourage such behaviour. This will diminish British sovereignty, and place the interests of British businesses and the liberty of their personnel in jeopardy, as countries with legal standards and traditions very different to our own seek to assert their own laws. It will certainly act as a barrier to free trade and free movement, as foreign businesses are deterred from placing their assets and personnel within the reach of enforcement, and British businesses do likewise when foreign countries reciprocate.

4. The UK, most than most countries, benefits from the thriving Internet sector. More than most, Internet-led innovation is leading economic transformation and consumer benefit. We therefore stand to lose more than most if this spirit is stifled by the need to comply with a range of foreign law, including laws intended for blatantly anti-competitive purposes, predicated on the assertion that merely being accessible by the citizens over the Internet is sufficient to place our businesses under their authority.

Secrecy regarding communications data

5. The Draft Bill introduces new secrecy provisions. While RIPA 2000 already had tight provisions governing the secrecy of interception capabilities, these have been extended to cover new areas. Under the Data Retention Directive and its temporary replacement the Data Retention and Investigatory Powers Act, the data types ISPs were required to retain were visible on the face of legislation. Under the Draft Bill, by contrast, a telecommunications operator must keep secret what they are required to retain and indeed the very existence of a retention notice.
6. We recognise the importance of protecting operational security and agree that legal restrictions should be placed on telecommunications operators preventing them from "tipping off" the subject of investigations. We also agree that is would be irresponsible to disclose certain details relating to investigation capabilities, in particular weaknesses in or limitations to more general capabilities that are more widely expected. That said, we do question whether it is healthy for the democratic process to conceal the overall picture of the state of general surveillance of the population in the UK from Parliament and the courts[940].

Interception without a warrant

7. Under RIPA, actions by telecommunications operations that would otherwise constitute an unlawful interception are authorised if they are a necessary part of the provision of the service[941].
8. This is necessarily preserved in the Draft Bill[942]. However, the Draft Bill also provides new cases where a telecommunications operator is authorised to intercept without a warrant: for the purpose of any enactment, or for the purpose of "preventing or restricting the viewing or publication of the content of communications transmitted"[943].
9. Essentially, this removes the legal impediment to ISPs from conducting Deep Packet Inspection (DPI) so as to inspect customer traffic and decide whether to block it.

[940] We note that the government disfavours the term "mass surveillance" when applied to the data retention regime. For clarity, we are referring here to the intention to collect and record, at minimum communications data relating to every electronic communication made in the UK, without requirement for prior suspicion that any of the parties to the communications is involved in an offense or anything else of interest to the public authorities. We consider that that is sufficient, by itself, to justify the use of this terminology. We not mean to imply that the population as a whole will have their data examined by a human being, and we understand that the contents of communications are not collected by measures that apply to the UK population as a whole. Any further intrusion that may or may not be introduced by this Draft Bill (such as continuous geolocation tracking, or automated profiling through the "filtering arrangements") we consider merely supplementary forms of surveillance.

[941] See RIPA 2000, s3(3).

[942] See s33 of the Draft Bill, in particular s33(2)(a)

[943] See s33(2)(c)

10. This restriction in RIPA has previously been a reason why ISPs could not accommodate informal and political government requests to block access to certain content; ISPs have told Ministers that if they wish ISPs to do this, they will have to legislate as by virtue of the legal prohibition on unlawful interception ISPs cannot comply voluntarily.
11. We note does not only enable the blocking of content which is illegal to possess (mainly, child abuse imagery and certain terrorist content), which is illegal to publish, or which is not illegal to publish but which may give rise to a civil complaint; it also enables the blocking of content which is lawful for all purposes (but presumably, may be disfavoured nonetheless).
12. We also note that this clause is not necessary to enable blocking with the consent of the customer, which already occurs.
13. Some of our members would welcome this restriction being lifted, so that they are able to assist the government in carrying out its policy. Others would regret it, as they do not wish to come under greater government pressure to censor Internet content informally, without a clear statutory basis.
14. As our members have differing views, we cannot make a clear recommendation of our own. We simply advise the Joint Committee that the purpose of this clause is to enable the introduction of new categories of Internet blocking without the need for further legislation.

Catch-all powers and encryption backdoors

15. We are concerned about the breadth of powers contained in ss188-190, and of their likely use and effect.
16. The national security notice in s188 appears to be all empowering. We make no legal submission as to whether it meets legal standards that require compulsory powers to be legally foreseeable, but it certainly does not seem to us to meet the spirit of such requirements. We think Parliament should more tightly specify the powers it grants to the executive.
17. We are also concerned about the breadth of the technical capability notice contained in s189.
    a. Here we get the sense that the government has started with the (already very broad) s12 RIPA 2000, which allows the Secretary of State to order a telecommunications operator to do anything required to maintain an interception capability, and generalised it by removing the limitation to an interception capability. What is left is a requirement "to provide facilities or services of a specified description"[944], where "specified" means specified by the Secretary of State in the notice.
    b. Again, we think Parliament should more tightly specify the powers it grants to the executive. Telecommunications operators ought not to be exposed to a general requirement of servitude.
18. In s189(4)(c) there is a reference to one of the obligations that may be imposed on a telecommunications operator being "the removal of electronic protection applied by a relevant operator to any communications or data".

[944] See s189(4), especially s189(4)(a)

a. This particular provision has been the subject of much press comment and speculation; some of it no doubt ill-informed, but some of it carrying the air of a government background briefing.
b. It is suggested that this phrase in particular, and s189 in general, is intended to empower the Secretary of State to require telecommunications operators to provide "backdoor access" to their services, bypassing encryption that normally protects customer communications.
    i. For example, Apple Facetime is a audio- and videoconferencing service. While customer data passes through Apple's servers, to protect confidentiality and assure customers of the integrity of the service, all such data in encrypted in a manner that it can only be decrypted by other parties to the call; even Apple does not have access to the content. This is known as "end-to-end encryption"; only parties at the "ends" of the communication have the decryption capability, and not anybody in the middle (such as Apple, in this example).
    ii. The suggestion is that by notice under s189, the Secretary of State could order a telecommunications operator like Apple build in to the design of their product a "backdoor", to ensure that they, as well as parties to the call, also have the ability to decrypt the communication.
c. End-to-end encryption is fundamental to network security, and the promise of end-to-end encryption in a product like Apple's Facetime service is essential to its viability in the market.
    i. There are many other communications and data storage services that are designed in the same way and depend, for their market viability, upon the same assurance.
    ii. This is not mainly because customers want to be protected against eavesdropping by the law enforcement and security services, but because they do not wishes to be exposed to the risk of compromise by either (a) the telecommunications operator acting deliberately, for its own ends or (b) any person who is able to unlawfully compromise the security of the telecommunications operator.
    iii. We are not certain whether this power could also be used to require a similar backdoor to be built into data storage services, such as Amazon AWS, Google Glacier and so forth. Indeed, we doubt such a provision could ever really be enforced. However, we are completely certain that corporate users of "Cloud-based" data storage depend upon the effectiveness of encryption to meet their own legally-binding security needs, and that any attempt to expose corporate data to inspection by the cloud provider strikes at the heart of the business model.
    iv. We also wonder what effect this could have on software developers. In principle, a software developer is not, by virtue of that face, a telecommunications operator, and so not subject to a notice under s189. However, we wonder what the result would be if, in receipt of an order as described, instead of building a backdoor into the encryption in Facetime, Apple instead altered the design so that Facetime calls no longer traverse Apple's servers. Could a s189 notice

prohibit that? Could a s189 notice prohibit Apple from introducing a "new" service with that design? This is not clear.

d. Strong encryption is essential to technical security and business confidence. The threats the UK faces lie more with security weaknesses than excessive strength. While we understand that investigations may sometimes be impeded by the existence of strong end-to-end encryption, on balance its use should be encouraged, not eliminated. There will usually be an alternative route to pursue an investigation, but there is no alternative to strong encryption if the Internet is to be any better than woefully insecure.

Part 4: Data Retention

Internet connection records

19. The collection of Internet connection records does in our view constitute an expansion of the intrusive effect of data retention compared with existing arrangements.
20. We are aware that the Joint Committee is investigating whether it is possible to distinguish between the content of the communication and an Internet Connection Record.
21. We believe that while the Draft Bill can and does make a legal distinction that is capable of being implemented and adhered to, we have serious doubts about whether it is possible to align that distinction with the distinction between "merely identifying a technical system that was accessed without disclosing any meaning from the communication itself" and "disclosure of facts or clear implications about the nature of what was being communicated".
22. Consider, for example, the following illustrative example.
    a. Internet Connection Records might show that a user had repeated access over a period to the following web sites:
        i. http://www.thewhiskeyexchange.com/
        ii. http://www.masterofmalt.com/
        iii. http://www.liqor.com/
        iv. https://uk.thebar.com/
        v. http://alcoholicsanonymous.com/
    b. We do not see how it is possible to see such a pattern of access without inviting the inference that the user may have, or suspects they might have, a drinking problem.
23. LINX does not have a view on whether this additional intrusion is justified: that is a matter for Parliament. We would caution the committee, however, not to assume that the effect of analysis of communications data patterns is either minor or rare. A much greater proportion of people's lives are lived "online" than when Parliament last legislated with full legislative scrutiny, RIPA 2000, meaning there is a much richer range of communications data to be had. Further, enormous progress has been in recent years in analysing large data sets to draw such inferences, especially in drawing statistically valid inferences that may not be at all apparent from the data itself.

The impact of the definitions of certain terms

Communications data and third party data

24. We are concerned that, contrary to direct assurances the Home Secretary gave to Parliament, the terms of this Draft Bill would authorise the Secretary of State to impose requirements on Internet access providers (ISPs) to collect third party data.
25. When consulted on the Draft Communications Data, the requirement to collect third party data contained therein was one of the primary points of concern for us and our members. We considered that the practice would be extremely (and expensive) difficult to implement. Without drawing a conclusion as to whether the additional intrusion was justified, we noted that far from being a mere updating and continuation of existing requirements (as the government contended) the collection of third party data by ISPs would constitute a "*substantial extension of their duties that is, in our opinion, materially distinct from existing data retention requirements, amounting to a complete novelty*".
26. Our concerns were shared by others:
    a. The conclusions of the Joint Parliamentary Committee on the Draft Communications Data Bill regarding third party data were
    The Home Office knows that not all overseas CSPs will comply with retention notices. It is for this reason that the notices issued under the order-making powers in clause 1 may require UK CSPs to keep third party data traversing their networks. ***UK CSPs are rightly very nervous about these provisions.*** *The Home Office has given an oral commitment to UK CSPs that the Home Secretary will invoke the third party provisions only after the original data holder has been approached and all other avenues have been exhausted. The Home Office has also given a commitment that no CSP will be asked to store or decrypt encrypted third party data. These commitments should be given statutory force.* (Paragraph 109, emphasis added).
    b. David Anderson QC, the Independent Reviewer of Counter-Terrorism Legislation, said in his report "A Question of Trust"
    c. There should be no question of progressing proposals for the compulsory retention of third party data before a compelling operational case for it has been made out (as it has not been to date) and the legal and technical issues have been fully bottomed out.
27. The response of the government has been to introduce a new concept in this Draft Bill, "Internet Connection Records".
    a. Internet Connection Records appear to be records of which websites (or other Internet-based service) a user has visited, but do not includes details of what they have done using that service.
    b. To take an illustrative example, consider a person who is a BT Internet-access customer who uses Facebook to send a message to another person. Requiring BT to collect third party communications data would require BT to collect details of that message including, *inter alia*, the fact, time and recipient of the message. By contrast, collecting Internet Connection Records would only

require BT to identify and record that their user had visited, at a given time, the Internet Protocol address that is used by Facebook.

c. Government and media commentary has since focused on Internet Connection Records, and the government has attempted to make the operational case for their collection.
d. Collecting Internet Connection Records is represents a substantial increase in the duties of ISPs compared to the current arrangements. It will certainly be expensive, and while technically feasible it will frequently require the installation of new equipment the support of which will constrain future networks design. This will impose additional costs and opportunity costs on ISPs that are not readily calculable and so are unlikely to be recoverable even if the government reimburses ISPs for the full capital costs and ongoing direct operational expenses.
e. Nonetheless, it must be recognized that the technical challenges and costs of collecting Internet Connection Records, significant though they are, pale in comparison to the extraordinary challenge inherent in collecting an arbitrary range of third party communications data.

28. Government positioning, media commentary, the impact assessment and the nature of the distinction between Internet Connection Records and third party data combine to invite us to leap to the conclusion that a compromise has been reached: that the government has been persuaded to make ISPs take a big step forward (to collect Internet Connection Records) rather than a giant leap (to collect third party data).
29. LINX is concerned that such an inference is not supported by the wording of the Draft Bill.
    a. "Internet Connections Records" appears in the Draft Bill in Part 3, which concerns the procedures for public authorities to access records of communications data held by communications services providers (CSPs). Special provisions are made where the data being sought matches the definition of an Internet Connection Record.
    b. The requirements on CSPs (including Internet access providers) to collect communications data are found in Part 4 of the Bill.
    c. Part 4 contains no reference to Internet Connections Records at all. Instead, it grants the Secretary of State a power to impose tailored requirements on individuals CSPs to collect "relevant communications data". The Secretary of State appears to have complete discretion as to what types of data she may require CSP to collect, provided that it falls within the extremely broad range covered by s71(9) and constitutes "communications data" within the meaning of s193(5).
    d. We do not see anything in Part 4 of the Draft Bill or elsewhere
        i. That would limit the data to be collected to data that already exists; or
        ii. That would limit the data to be collected to data relating services provided by the same telecommunications operator as the telecommunications operator collecting it[945]

[945] To assess this requires a very careful reading of s193(5). As far as we can tell, the "telecommunications service" does not need to be provided by the same "telecommunications operator" as the telecommunications operator doing the collection.

30. We therefore do not think that the collection and retention requirements that the Secretary of State would be authorised to impose are limited to Internet Connection Records, but could include the collection of third party data.
31. We reiterate our concerns that collection of third party data by ISPs would be technically extremely challenging, immensely costs, and would amount to a considerable increase in the level of intrusion into the lives of ordinary Internet users and the confidentiality of commercial communications. We also note that while the government has made its case for the collection of Internet Connection Records, it has not attempted to make an operational case for the collection of third party data.
32. If it is Parliament's intention that ISPs should be required to collect Internet Connection Records but should not be required to collect third party data, we believe the definitions of "relevant communications data" and/or of "communications data" need to be tightened considerably.
33. At the very least, even if our reading of the definitions is wrong, we think they should be very much more clear on such a crucial point than they are in this Draft.

Entity data

34. Communications data is divided into "events data" and "entity data". Events data means data about a network event, such as data about a communication. Entity data cover everything else that a telecommunications operator knows about anyone else, or about the relationship between themselves and that other person.
35. This is an exceptionally broad definition.
36. The definition of entity data has its roots in "subscriber data" under the Regulation of Investigatory Powers Act 2000 (RIPA).
    a. "Subscriber data" meant, loosely, information that the telecommunications operator held about their customer. Back when RIPA was passed, the information telephone companies held on their customers was the customer's name and address, and other relatively unintrusive information regarding the services taken and billing.
    b. "Entity data" has broadened that definition so that it no longer only refers to customers. More particularly though, the changing definition of who is a telecommunications operator means that the nature of the information described has changed enormously.
37. Amongst the types of companies that now fall within the new definition of a telecommunications operator as social networking sites and online messaging services. This means that Apple, Facebook, Google, Microsoft, Yahoo! and others will all be considered telecommunications operators within the meaning of the Draft Bill. And everything they know about anyone will be considered "entity data", other than that which is events data.
38. Accordingly, the power to require telecommunications operators to give access to communications data includes access to anything that Google, Facebook and Apple hold on anyone[946].
39. Given the breadth of information covered, we find it remarkable that the Draft Bill does not make any attempt to segregate different types of entity data or make

[946] We assume here full compliance by these companies. For reasons of lack of jurisdiction, that may not necessarily occur. But the Draft Bill is intended to apply to these companies extraterritorially.

differential provision for access according to the level of intrusion. We consider this inconsistent with the continuation of a much higher level of protection for the content of communications than for communications events data. Entity data will often be as intrusive as communications content, and will in many cases reveal exactly the same information.

Location data

40. s71(9) describes the types of communications data that telecommunications operators may be required to retain by a retention notice issued under Part 4.
41. By virtue of s71(9)(f) one of those types is location data[947].
    a. In relation to a fixed line telephony or Internet service, this means the location where that service is provided, such as a consumer's home.
    b. In relation to a mobile telephony or Internet service, or to any Internet communication that was made using a mobile device, this means the geolocation of that device at a given moment (in the case of an Internet communication, the geolocation of the device at the time the communication occurred).
42. We would like to draw to the attention of the Committee:
    a. Modern smartphones are typically in near-continuous communication, provided data service is activated, as Apps running in the background update their data: checking for new mail, updating weather reports, loading news stories and accessing the myriad of other services Apps provide. Each and every communication between the device and a server (for example, every time it polls a server to see if new mail is available) constitutes a communications data event, and the location data relating to that event is the location of the mobile device at that moment.
    b. Modern smartphones also include advanced mechanisms to determine their current location. Sophisticated algorithms combine at least three sets of potential location clues to help calculate an accurate position
        i. GPS satellite positioning information (where available);
        ii. The list of unique identifiers for communications access points (Wi-fi and mobile cell-site) that are visible to the phone are sent to the phone's location services provider (typically Apple, Google or Microsoft) together with strength of signal information; the location services provider combines that with its own information on the locations where those access points are visible (and possibly the last-known location of the phone) to estimate current position.
        iii. Finally, when the phone can uses its built-in accelerometer to complement "last known" positions using dead-reckoning.
        iv. Note that the location services provider is also a telecommunications operator within the meaning of the Draft Bill, and that each time the phone uses the location services provider to ascertain or improve its understanding of its own location, that is itself a communications event.

[947] See also Example 2 in Paragraph 137 of the Explanatory Notes

c. We do not wish to go into detail concerning the accuracy of the current capabilities of mobile phone networks; suffice to say that if geolocation data from the phone were retained and made by available those entities such as Apps services (who will be deemed telecommunications operators within the meaning of this Draft Bill, but were not under RIPA 2000) then accurate tracking of the UK population will be very much enhanced compared with pre-existing norms.

43. We consider it a matter for Parliament to decide whether it is proportionate and appropriate for telecommunications operators to be required to keep near-continuous and potentially substantially complete geolocation records of the movements of essentially the entire population of the UK. LINX's role is simply to assist the Joint Committee by pointing out that that is the implication of the Draft Bill under consideration.

Part 3: Authorisations for obtaining communications data

44. We note that it is proposed under s46(1)(b)(ii) that one of the purposes for which a designated senior officer may authorise obtaining communications data is the "purposes of testing, maintain or developing equipment, systems or other capabilities".
45. We are of the opinion that it is not normally considered good practice to do systems development using live data: to reduce the risk of security breaches, dummy data is used. We also note that permitting the use of such data for the purpose of "developing …other capabilities" would allow, under the guise of such development, analysis of data in ways that would not be authorised elsewhere. We would not want to see the creation of a loophole that enabled a semi-permanent "development platform" that bypassed regular systems. We hope that this sub-section could be tightened up in final legislation.
46. The language of s47(4), with its double-negatives, is very difficult to follow, but it appears that these provisions do not apply when the material sought is not an Internet Connection Record.
47. We note that s50(2) makes it a duty of a telecommunications operator to minimise the data that needs to be processed for the purpose concerned. We are unclear what this means in practice, and in particular, how much and what kind of pre-processing the telecommunications operator will be expected to undertake in order to satisfy this requirement. Extensive pre-processing will increase costs.

Filtering arrangements

48. In our evidence to the Joint Committee on the Draft Communications Data Bill we said
"In our analysis the "filtering arrangements" provided for in clauses 14-16 are best understood as a "profiling engine" which creates detailed profiles on all users of electronic communications systems and makes those profiles available for sophisticated data mining.

In our opinion this profiling engine amounts to an enormously powerful tool for public authorities. Its mere existence significantly implicates privacy rights, and its extensive use would represent a dramatic shift in the balance between personal privacy and the capabilities of the State to investigate and analyse the citizen."

49. In our view the filtering arrangements in this new Draft Bill would also have this effect.
50. As with the Draft Communications Data Bill, we do not express an opinion as to whether such a shift is justified; it is for Parliament to make the basic value judgement as to the appropriate balance between personal privacy and the public interests of the State. However, we believe that Parliament should be aware of the enormous analytical power that this capability represents for profiling individuals (and potentially, the population at large).
51. We do not agree with the government's characterisation of this portion of the Draft Bill as a safeguard that minimises the intrusive nature of access to communications data by reducing the volume of data that will be released to investigating officers. We think a much more accurate characterisation would be to regard these arrangements as an enormously powerful and intrusive new investigatory tool that brings the power of Big Data analysis to law enforcement investigation on an unprecedented scale.
52. In a simple case, the use of this profiling engine could have impressive results in improving policing efficiency and effectiveness. For example, consider an investigation into cases of public disorder and other offences at a political protest which had turned violent. A straightforward query of the profiling engine could ask "Please supply the names and addresses of every mobile phone users whose phone was located in Trafalgar Square between 3pm and 4pm on Saturday 31st October – but only those who had also, via their mobile phone or a via fixed-line ISP account registered in their name or at the same address, accessed the web site www.protest.org during October". Combined with a request to Facebook "Please supply the names of all the people who, during the last month, directly sent messages to or received messages from [any of the people on the previous list" and the filter again "Please supply the names and addresses of every mobile phone users whose phone was located in Trafalgar Square between 3pm and 4pm on Saturday 31st October – but only those who appear on this list [received from Facebook]", the protestors could all be quickly and easily rounded up for questioning, while segregating them from ordinary tourists and others who were merely there by happenstance.
53. The preceding example is simple, because it only asks for a single piece of data to be reported (the name and addresses of the user(s) of particular mobile phone(s)), albeit data discovered at the end of a chain of cross-referencing. If instead multiple pieces of data are reported, the report could, taken as a whole constitute an analytical tool in its own right.
54. It is evident that to make effective use of communications data reports that return multiple data points a considerable amount of post-processing would be required.
    a. This is most evident in the case of geolocation data: a string of GPS coordinates is essentially unintelligible to a human being, but starts to become useful when plotted on a map and labels corresponding to time are added to locations; this becomes more useful still when cross-referenced

against other (external) data, indicating (for example) “this region on the map indicates Heathrow airport: did the target enter that region?” (a technique known as “geo-fencing”).

b. However given the sheer volume of communications data available, we would expect extensive use of processing in most cases, to avoid investigators being overwhelmed.
c. It is not wholly apparent from the Draft Bill whether the “filtering arrangements” run by the Secretary of State would perform sophisticated post-processing of the data and cross-referencing with external data, so as to make it meaningful and useful. However for the purpose of assessing this legislation it seems immaterial whether this is done centrally by the Secretary of State, or whether (essentially unintelligible) raw data on the target is received from the filter and then fed into an analytical system operated by the investigating agency, once the “filtering arrangements” have reduced the data to a sufficiently contained set to be susceptible to such analysis.
d. Even a simple count could be useful in reducing extraneous data and intrusion:
    i. Consider an investigation into terrorist offences, where the target has been identified as an associate of a suspect, but not yet a suspect themselves. The request “Please give me a list of each website accessed by our target during the last three months, and the date and time of each” is likely to return a huge volume of information to sort through, as well as revealing much irrelevant material. It might also be considered a disproportionate enquiry. As an alternative “Here is a list of websites we are worried about. Please say which, if any, our target has visited, and if any, on how many occasions in the last three months did he visit each one?” would result in a much smaller, simpler list that would help investigators add the target to, or eliminate the target from, the list of suspects. It might also be more likely, as a result, to be deemed to be a proportionate enquiry.
e. A simple count of visits to web sites of interest may not by itself be sufficient to safely designate a target as a suspect or in the clear. Multiple factors would likely be considered: not just web sites of interest but also, for example, how many suspects does the target associate with? Taken individually, this is a core aspect of investigative operations. Combining the responses, however, the results can build up a score:
    i. For each visit to any website on list A, score 1.
    ii. For each visit to any website on list B, score 5.
    iii. For each visit to any website on list B after the fifth visit in the month, score 10.
    iv. For each direct communication with a person on list C, score 10.
    v. For each communication with a person who has communicated with a person on list C in the past month, score 1.
f. A communications data report on a person could, therefore, in principle look rather similar to, and form a close analogy with a consumer credit report, complete with a “risk factor” score analogous to a consumer credit score, but tailored to the purpose of the investigation.

55. When used in a targeted fashion, against persons already of interest who would otherwise come under intrusive investigation anyway, this kind of technique might be considered to be both proportionate and the help minimise unnecessary intrusion.
56. However, we note that it is the purpose of this legislation to keep voluminous, intrusive and potentially intimate records on the entire population. Will it also be used to *score* the entire population for potential to have been involved in a crime, or other permitted areas of enquiry? If so, will such scores only be used to eliminate suspects for an acknowledged crime, or might they also be used to detect where a crime might have taken place?
57. We do not think the nature of the data is such that scores could only be constructed to support investigations into the most serious matters such as terrorism. Consider, for example, how a communications data report might assist an investigation by H.M. Revenue and Customs into whether the target's lifestyle matched their reported income.
    i. A full set of geolocation data tracking the target's every movement would be enormously helpful: this would certainly identify the number of nights spent away from home so as to estimate the number of holidays and away-breaks taken. With accurate geolocation data it would be possible to identify particular hotels (enabling assessment of their cost from public information); it may also be possible to identify the target frequenting establishments where substantial discretionary spending is conducted in cash, such as restaurants, racecourses, betting shops, nightclubs and strip clubs[948].
    ii. Even without accurate geolocation data, given the ordinary use of the Internet in modern society, it may still be possible to identify the target as having visited such locations (e.g. by when the target accesses on-premises wi-fi), or by simple inference when he connects to the establishment's web site to check its address[949].

Part 5: Equipment interference

58. We do not doubt that there is a strong operational case for law enforcement authorities and the security and intelligence agencies to be given powers to conduct certain types of equipment interference in certain types of situations. However, we are greatly concerned that the sweeping powers envisaged in the Draft Bill fail to provide the necessary mechanism to prevent their use from result in serious harm to the security of UK critical infrastructure.
59. Equipment interference could be envisaged in a wide variety of scenarios, with strikingly different risks and consequences:
    a. We do not doubt that there is a strong case for allowing law enforcement officers to interfere with computing devices that are in their physical possession as a result of being seized from a suspect, in order to obtain

[948] It is worth remembering that perfect accuracy is not necessary for such purposes; collect sufficient data and you can proceed on the basis of statistical probability. In such a case, it would assist an investigator if the target frequented a variety of different strip clubs, rather than had a favourite.

[949] The fact that the target was using the establishment's web site to check its street address would not be evident from the communications data: this is content. Nonetheless one could establish that the target was interested in horseracing (or strip clubs), and that may be sufficient for the investigatory purpose.

information from the device. We understand that existing powers under the Police Act already provide for this.

b. Similarly, if such a device has stored data on a "cloud service", we do not doubt the necessity or proportionality of using the credentials stored on the device to access that data.
c. Making changes to data on such a device or service, or using either of them to send communications impersonating a person who is not a law enforcement officer does create at least the risk of damaging the integrity of evidence, or of creating material that ought to be evidence. We assume that there are separate provisions covering the disclosure of relevant material to criminal defence teams (or, in non-criminal matters such as some investigations by the FCA or HMRC) others similarly situated.
d. Nor do we see a material distinction between using a seized device to access an account it has on a cloud service, and using access credentials to that service obtained by other means.
e. We do, however, see a clear distinction between these cases and exploiting a software flaw or design vulnerability in the security of a remote computing system.
f. Exploiting such security weaknesses inherently harms the system concerned, the entities that own and operate the system concerned, and anyone that relies upon it.
    i. Such exploitation undermines trust and confidence in a variety of ways, but most comprehensively, once it is known that a system has been compromised it is impossible to trust the integrity of the system or any data it has processed.
    ii. Any such intrusion certainly risks causing additional, direct collateral damage, both to the system itself, to data stored upon it or processed by it, and to any systems that rely upon it.
    iii. In particular, exploiting one security vulnerability so as to create a new one or otherwise enhance the accessibility of the system exposes the system to significant risk that the system will also be compromised by unknown third parties, acting without lawful authority.
g. When deciding whether to run these risks, it is clearly important to consider the nature, ownership and use of the system in order to consider the possible impact of intended or unintended consequences of interfering with it.
    i. Where the owner/user is a target whose interests have reduced weight (for example, a terrorist suspect) and the system is one not widely relied upon (for example, that suspect's personal computing device) it may be easy to come to the conclusion that any unintended technical consequences from hacking into it are both unlikely and of low impact, and so an acceptable risk.
    ii. By contrast, where the target is an entirely legitimate organisation (such as a telecommunications operator or a financial institution), and the system is one which is widely relied upon, or which is a critical input to something widely relied upon, the risk calculus is completely different.

iii. In some cases, the consequences of impairing a system could cause severe financial damage or threat to life or health.

h. In particular, we would stress to the Committee that any such attacks on systems that constitute infrastructure may have unpredictable, and severe, consequences: while the public authority concerned may believe they can assess the technical risk, they are most unlikely to be capable of assessing potential impact.

i. We do not like to conjure catastrophe scenarios, but we invite the Committee to consider the possible consequences if interference with a piece of telecommunications infrastructure accidentally exposed it to the control of some teenage vandal or resulted in temporary loss of service or it corrupting data, and that corrupted device, unbeknownst to the security service was also relied upon by a security or medical monitoring service, a hospital, a traffic control system, a water purification plant or any of a myriad of other critical systems.

ii. Of course, it is easy to say that no such system should be critically exposed to a single device in such a way. But that does not mean that they will not be: we frequently find that things are not as one would wish. Moreover, even when conducting contingency planning, the operators of critical systems must focus on risks that are controllable for them: hacking by law enforcement and intelligence agencies under this Bill does not fall into this category. So while a critical service may have protected themselves against loss of availability of a communications service, they may be entirely unprotected if the integrity of that service is compromised and begins sending corrupted data or –worst of all- unauthorised commands.

60. We would therefore like to stress to the Joint Committee the difficulties that will be encountered in performing any risk assessment for a proposal to interfere with a device that is part of a business operations system, rather than an end-user device

a. when hacking into computer systems run by infrastructure businesses the upper boundary of potential impact when causing damage to or exposing an additional weakness in a critical system can reach as far as sheer catastrophe;

b. it is very difficult for an outside organisation, even an intelligence agency or law enforcement authority, to assess the worst-case scenario in a given instance (indeed, our work on critical infrastructure planning has taught us the challenge even the operator has in conducting such an assessment);

c. it is also very difficult for an outside agency (and sometime even the owner) to properly assess whether a given business operations system is critical to a critical infrastructure service;

d. indeed, in our increasingly interconnected world, critical inputs to critical systems can be operated by outside suppliers;

61. Given the potentially serious consequences in some cases, and the great difficulty in assessing whether those consequences might be at risk in a particular case, we would consider that it would often be reckless to compromise business operations systems, and in particular to compromise business operations systems of telecommunications operators.

62. Nor do we consider it necessary for law enforcement or the security and intelligence agencies to hack into the operational systems of telecommunications operators in any but truly exceptional circumstances: there are wide powers to compel their cooperation.
63. We note with dismay the following omissions from Part 5 of the Draft Bill:
    a. There is nothing that seeks to distinguish between interference with systems used by suspects and those used by innocent parties;
    b. Apart from the bare (and non-specific, and undeveloped) legal concept of proportionality, there is nothing
        i. that seeks to identify or protect the interests of legitimate users of the systems that are interfered with; or
        ii. that requires specific assessment of the potential impact of the interference on critical services.
    c. There is no obligation on the authority conducting interference to "clean up" after the conclusion of their operation, for example by removing malware they have installed or correcting additional security vulnerabilities they have introduced into the system. Indeed, if considered as an additional interference that would not be for the specified purposes[950], the terms of the Draft Bill may actually prohibit such clean up.
64. We do not doubt that statute law should provide a limited set of powers that enables appropriate authorities to conduct defined types of equipment interference in carefully defined circumstances.
65. In our view Part 5 of the Draft Bill does not achieve this: it provides a power for appropriate authorities to conduct any type of equipment interference in almost any circumstances they deem useful for the prevention of detection of serious crime, or other specified purpose, with no consideration for any other legitimate interests beyond the bare and unsupported assertion that the warrant issuer deems it proportionate. We consider that on balance this will be detrimental to the security of the United Kingdom.

Part 8: Safeguards; the inadequacy of the "proportionality" test

66. The approach taken in this Draft Bill, as in the Draft Communications Data Bill, is to record an enormous volume of data on essentially every person in the country, regardless of whether they have ever been a person of interest, in case they might ever be a person of interest in the future, and to control only through an authorisation scheme that focusses on three elements:
        i. Whether the person using the power is a person who can be authorised, and whether they have been authorised by someone capable of authorising them;
        ii. Whether the purpose for which they wish to use the power is one identified in the Draft Bill; and
        iii. Whether the use of the power in this instance is proportionate.

    This is backed up with an inspection regime.
67. There is, however, very little specificity as to *how* the powers can be used.

[950] The purposes specified in s81(4), s86(1)(b), s87(1)(a), or s89(1)(a), as appropriate to the warrant

68. The purposes for which the powers can be used can be quite broad
    a. The Bill provides powers to obtain communications data (including use of the filtering arrangements/profiling engine) are made available for the purposes including detecting all crime, not merely terrorism nor only serious crime (some of the other powers are limited to serious crime).
    b. These powers are only available for a specific investigation or a specific operation[951], but while "detecting crime" is defined as including "establishing by whom, for what purpose, by what means and generally in what circumstances any crime was committed, and the apprehension of the person by whom any crime was committed[952]" the definition is not limited to those purposes. In particular it is not clear as to whether they are also available for discovering whether a crime has taken place, or even whether there is any reason to suspect that one might have taken place.
    c. The same powers are available for the prevention of crime. No particular provision is made for how close a nexus there needs to be to an actual possibility of an actual crime. Notwithstanding s46(b)(i), there is, for example, no limitation on the use of the powers for the prevention of crime to circumstances where a specific crime is in the contemplation of the investigating officer; the specific operation in question could be an operation to reduce the general prevalence of a particular type of offence.
69. If Parliament is not to specify how particular powers can be used in any great detail, and the purpose of the powers is so broad, very great weight is placed on the mechanisms for ensuring in individual cases that there is good judgement as to what is proportionate.
70. In this context, the Draft Bill is remarkably lacking statutory standards or guidance to support the assessment of proportionality, to ensure that such decision-making comports with Parliament's own view of what it proportionate.
    a. For interception there is the "double lock", whereby Judicial Commissions must (normally) approve warrants, which includes the Judicial Commissioners taking a view as to the proportionality of the warrant. However the Draft Bill would not burden the Judicial Commissioners with any statutory standards, principles or guidance to apply in deciding whether a particular warrant before them is proportionate.
    b. For access to communications data
        i. The designated senior officer must consider whether the request is proportionate; and
        ii. The designated senior officer must consult a single point of contact, who may advise (but not decide) on the lawfulness of the request, which could include advice on its proportionality;
        iii. In the case of an authorisation for the purpose of confirming a journalistic source, the approval of a Judicial Commissioner is required But the Draft Bill provides neither the designated senior officer, the single point of contact or the Judicial Commissioner with any statutory standards, principles, or guidance to apply in assessing the proportionality of the request for authorisation under consideration.

[951] s46(b)(i), in relation to operations; the powers are also available for testing and development, see s46(b)(ii) for details
[952] s195(2)

c. For equipment interference, there is again a complete lack of statutory standards, principles, or guidance for the warrant issuer to apply in assessing the proportionality of the request for authorisation under consideration. We discuss this in more detail in the section of our submission on equipment interference.

71. The Investigatory Powers Commissioner has a duty to keep the use of these powers under review, and to make reports to the Prime Minister which (after redaction) are to be published and laid before Parliament.
    a. These reports could include discussion of the principles for proportionality, but need not do so.
    b. In fact, the Draft Bill lays on the Investigatory Powers Commission has specific duties to law enforcement and security interests[953]. Unless more specific duties are laid upon him requiring him specifically to consider and report on the proportionality of practices and capabilities under review (including, especially, new practices and new capabilities) the Commissioner's duties to law enforcement may well inhibit him from transparent reporting. In particular, he may feel inhibited reporting on and bringing to Parliament's attention any practices that, while well-intentioned, Parliament might consider to have crossed the line into disproportionality.
    c. In any case, the Investigatory Powers Commissioner is, like everyone else with duties under this Bill, bereft of statutory guidance or statutory principles to apply in considering the proportionality of the matters he is supposed to keep under review.

21 December 2015

[953] These are duties to avoid acting in a way contrary to the national or prejudicial to the national security, the prevention or detection of serious crime or the economic well-being of the UK, under s169(5), and to avoid jeopardising the success of an intelligence, security or law enforcement operation, under s169(6)

Christopher Lloyd—written evidence (IPB0056)

Summary: Even if these monitoring measures are implemented, they are trivial to evade, even for the layperson. These evasion methods cannot be blocked or otherwise banned due to the nature of the Internet, as well as having multiple legitimate uses which are vital for everyday life and our economy.

The proposal is fundamentally flawed, and demonstrates a complete lack of understanding of the Internet. It carries serious moral considerations regarding privacy, it would be extremely costly to the taxpayer, put the public at serious risk of a data breach (see the recent TalkTalk hack), and would do nothing to stop any remotely competent terrorists or criminals.

1. The argument for encryption.

Many services on the Internet require encryption, and even if one completely disregards a British citizen's right to privacy, it is essential as part of a strong digital economy, allowing businesses to exchange and securely store information. Virtual Private Networks (VPNs) allow businesses to connect their regional offices over the Internet, and make it possible for employees to work from home by dialing into their corporate network. Online banking and many other services that require the exchange and use of confidential information also require encryption. When one connects via a web browser to a HTTPS site, such as a banking website, this also creates what is effectively a miniature Virtual Private Network.

For these to function it must be possible to securely connect so that no attacker may eavesdrop, intercept, or otherwise attack or manipulate the connection. Our economy, infrastructure, and technology is reliant on this.

A fundamental foundation of good encryption is that the encryption method must be secure. It is impossible to weaken encryption so only the "good guys" (like the police) can access it, while preventing any "bad guys" (like criminals) from doing so. If there is a weakness in the implementation, it can and will be exploited by criminals and terrorists. The only way of protecting against "bad guys" is to make the encryption unbreakable.

2. The ease of evasion.

To understand how flawed the proposal is, it has to be stated just how easy it is to evade these monitoring measures:

12. The TOR web browser is free, readily available, and takes no technical skill to use beyond being able to download and operate a regular web browser. It is no exaggeration to say a child could avoid monitoring in less than a minute.
13. Virtual Private Network (VPN) software is cheap and there are many options for users wishing to use such a service. VPN clients vary in complexity in their configuration, but are often designed such that a typical PC usercould make use of them with minimal knowledge and expertise. There are providers who offer VPN servers that lie outside the

UK, rendering them immune to any legal requests from the British Government, and many services would not hand over confidential customer information to a foreign government.

14. Due to content delivery networks (CDNs) being increasingly used on the Internet to deliver data in a more sustainable way (and help to protect web sites from threats like Denial of Service attacks), it is possible for terrorists and criminals to host web sites containing illegal content, which would not be flagged up by any monitoring efforts as the IP address will appear completely legitimate. The CDN would almost certainly not allow their services to be used in this way, but it would be very difficult for them to detect it without it being reported to them.
15. Legitimate sites can be used to communicate. For example, it is possible to encrypt and then upload a small file to Google Drive and share the link with a third party. All the ISP would see is that the user connected to Google, information which is utterly useless since millions of people use Google services each day. There are also many other legitimate file sharing websites which could be used to the same end. Such online "dead drops" are easy to use, and can be accessed so that even the service themselves -- who have far more information than the ISP -- do not know the contents of the file or the true identity of anyone accessing the file.
16. Information can be hidden in plain sight using deniable encryption methods such as steganography. For example, it is possible to hide a coded message in say a Facebook profile image with no need for direct communication. In online forums, "avatar" pictures could be set to send messages with no need for two profiles to directly communicate. Users could upload their own photographs. These are completely routine actions performed legitimately, and would appear no different from normal web browsing.
17. Communication can be achieved in unorthodox and arbitrary ways. For example two players could join a public server hosting an online video game and then spell out messages using bullet holes in the walls. Even if both players were monitored and had the information collated, it would look like two players playing a video game.
18. Due to the overhead and costs, smaller ISPs would have to be exempt. Criminals and terrorists can use smaller ISPs to evade monitoring.

3. Security of the collected information.

The collected information would be an extremely high value target for attackers, not only for blackmail material, but also because online activity reveals a lot about oneself. Even with a minimal footprint which only collects website domains and timestamps, it is possible to infer all kinds of private information. For instance, medical conditions, personal circumstances, sexuality, infidelity. This is information that a citizen has every right to keep private, where there is no strong "need to know" or "greater good" basis. This information would need to be stored in a very secure fashion. However, one only has to look at how often larger organisations are breached (and how little such breaches are punished) to understand this companies have a poor reputation for achieving this, and that given the size of such a target, this is very challenging.

4. The usefulness of the collected information.

As mentioned above, these measures are easily evaded by anyone competent. The information collected would be of little to no use for genuine law enforcement reasons or protecting interests of British citizens, but would put them strongly at risk of having their confidential, delicate, and sensitive information leaked, as such a database would be a very tempting target. This would ultimately endanger British citizens by putting them at further risk of criminal activity.

5. Privacy implications

For some reason, politicians seem to view the Internet as fair game for monitoring in a way that they apply to no other aspect of life or communications. No politican wishing to keep their post would ever dream of implementing such a measure where secret police open and monitor all letters, or record every phone call you make.

Online communications can be far more revealing even without detailed knowledge of contents, and implementing such measures sets the dangerous precedent that the state has the right to spy on innocent citizens for no reason, and that ultimately some of your innermost thoughts and private aspects of your life are the property of the state. This is against the principles and ideals in a modern democratic Western state.

6. Lack of technical understanding amongst politicnas

Politicians appear to have an extremely poor understanding of technology; this proposal would never have seen the light of day had Ms. May the slightest knowledge of how the Internet works.

The Internet is vital for life in the modern age, and such ignorance of the very basics of its operation should not be acceptable for any politician in today's world.

19 December 2015

Local Government Association (LGA), National Anti-Fraud Network (NAFN), Chartered Trading Standards Institute and Association of Chief Trading Standards Officers—written evidence (IPB0051)

1. About the Local Government Association (LGA)

1.1. The Local Government Association (LGA) is the national voice of local government. We work with councils to support, promote and improve local government.

1.2. We are a politically-led, cross party organisation which works on behalf of councils to ensure local government has a strong, credible voice with national government. We aim to influence and set the political agenda on the issues that matter to councils so they are able to deliver local solutions to national problems.

1.3. This evidence is submitted jointly by the Local Government Association (LGA), National Anti-Fraud Network (NAFN), Chartered Trading Standards Institute and Association of Chief Trading Standards Officers.

2. Summary

2.1. Although crime rates in general have continued to fall, rates of fraud increased by nine per cent between June 2014 and June 2015. Within these figures there was a 16 per cent increase in fraud related to on-line shopping and auctions as well as cold calling scams.

2.2. Local authorities have an important role in protecting consumers and businesses from these and similar types of criminal activity. Often those involved, like rogue traders and loan sharks, prey on the most vulnerable in society.

2.3. Teams within councils, such as trading standards, use communications data to tackle a range of criminal activity and fraud. It is therefore vital that the powers available to them keep pace with the technology through which an increasing amount of criminal activity is perpetrated.

2.4. Councils are not the primary users of communications data: the Report of the Interception of Communications Commissioner noted that councils were responsible for just 0.4 per cent of all notices and authorisations to access communications data in 2014.[954] However the ability to access this type of data is an important tool for local authorities to conduct their work.

2.5. The LGA and its partners support the powers set out in the Draft Investigatory Powers Bill, which maintain councils ability to access communications data under the new definitions of 'entity' and 'events' data. However, in amending the definitions of communications data, central government must ensure that there is

[954] Further information on the Report of the Interception of Communications Commissioner http://iocco-uk.info/docs/IOCCO%20Report%20March%202015%20(Web).pdf

full clarity about the types of data falling within each new category.

2.6. The importance of councils being able to access communications data is endorsed outside of local government. The Independent Reviewer of Terrorism Legislation (IRTL) concluded in a report last year that communications data is "properly and productively used… in combating a wide range of other crimes, most of them more prevalent than terrorism and some of them just as capable of destroying lives."

2.7. Additionally, charities such as Age UK also emphasise the need to ensure councils have the tools they need to investigate scams or fraud.

2.8. The LGA accepts the need for a range of safeguards to provide public reassurance that councils use communications data appropriately. Only 19 out of 6,000 (0.3 per cent) council applications to access communications data were refused by magistrates between 2012 to 2015. This confirms that the powers are being used proportionately.

2.9. In his recent report, the IRTL suggested that current safeguards are deterring councils from seeking access to communications data.[955] The LGA believes that although the existing safeguards should be maintained, there is a need to ensure that they are implemented in an efficient way that does not deter appropriate use of communications data.

2.10. Central government should ensure that councils are able to apply for and be granted magistrates approval electronically, in line with the recent Spending Review commitment to fully digitise the court system[956].

2.11. Central government should also consider the case for routing all such applications through a small number of magistrates courts with direct links to the National Anti-Fraud Network. By creating centres of expertise, this would ensure that this safeguard is applied consistently and robustly.

3. To what extent is it necessary for (a) the security and intelligence services and (b) law enforcement to have access to investigatory powers such as those contained in the Draft Investigatory Powers Bill?

3.1. Communications data is used by local authority trading standards teams to tackle scams and other activities that defraud businesses and consumers. This ranges from doorstep crime which targets vulnerable and elderly people to large scale cybercrime which is often conducted remotely. Corporate fraud teams in councils can use communications data to prevent fraud against local taxpayers, for example, tenancy fraud, right to buy fraud, social care fraud, insurance fraud and

[955] Further information on the Report of the Interception of Communications Commissioner: Paragraphs 9.99-9.100 https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf

[956] Further information on the Spending Review, paragraph 2.147 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/479749/52229_Blue_Book_PU1865_Web_Accessible.pdf

procurement fraud.

3.2. Charities who work with victims who are most at risk from these types of scams have endorsed the importance of councils retaining the right to access communications data. For example Age UK states: 'We know that scams are a huge and under-reported problem – recent ONS statistics estimated over 5 million incidents of fraud in a year. We also know that fraudsters target older people, exploiting those who live with dementia or are lonely. Some people are so lonely that they welcome the human contact in the scam letters they receive, not realising them to be fraudulent. In this context, trading standards officers have an essential role to play in protecting older people from scam mail. If we want to tackle this growing threat to people's wealth and health, we need to ensure councils have all the tools they need. Failure to do this means leaving older people open to continual attack and, ultimately, more pressure on the state, with victims who lose everything potentially needing health and care services and welfare benefits.'

3.3. Recent crime trends, specifically increasing rates of reported fraud, emphasise the need for councils to retain the ability to access communications data. Action Fraud, operated by the City of London Police, is the lead body for reporting fraud in the UK, and has collated information indicating that:

- One in four small to medium business enterprises (SMEs) fall victim to fraud every year. Last year alone fraud loss to SMEs was estimated at £18.9 billion.

- In the year ending March 2015, there were 230,000 fraud offences reported to Action Fraud. This is equivalent to four recorded offences per 1000 head of population. This is twice the rate of theft and four times the rate of robbery reported to the Police (information from Office of National Statistics).

3.4. Fraud undertaken via the internet is also increasing: we now shop, bank, date and access public services online, and as more of peoples' lives are conducted through the internet, so the opportunities to defraud people through it increase.

3.5. A Home Office Select Committee report from July 2013 noted that: 'The UK's crime statistics demonstrate that the incidence of e-crime is high and increasing…individual cybercrime victimisation is significantly higher than for 'conventional' crime forms. Victimisation rates for online credit card fraud, identity theft, responding to a phishing attempt, and experiencing unauthorized access to an email account, vary between one and 17 per cent of the online population for 21 countries across the world, compared with typical burglary, robbery and car theft rates of under five per cent for these same countries.'

3.6. The 2013 Norton CyberCrime report estimated that the cost of cybercrime in the UK in a single year was more than £800 million. As an example of the types of crime that can be perpetrated online, the National Fraud Intelligence Bureau identified that in 2014, £34 million was lost by victims of online dating fraud.

3.7. Both these reports outline the challenge of increasing rates of cybercrime. This needs to be addressed by enforcement agencies; and local trading standards teams have a critical role in doing so.

3.8. Communications data is used to build criminal cases against individuals accused of criminality and can be a crucial piece of evidence in: identifying the person owning an email or internet address or telephone number linked to criminal activity; proving that contact took place between the accused and the victim; or linking the accused to wider criminal networks. It can help to substantiate a prosecution case where records may not have been kept, or have been fabricated or destroyed, and where the alleged offender lies about their activities.

3.9. Alongside local trading standards teams, National Trading Standards (NTS) has also established regional and national teams that tackle regional and national level trading standards issues. Of these, the national e-crime and illegal moneylending teams and regional scambusters access communications data most often. Between April-December 2014, these teams:

- uncovered potential e-crime fraud of £14.6 million
- identified 546 illegal moneylenders with £905,000 of victim debt
- undertook activities that helped to avoid £134 million of consumer detriment
- received proceeds of crime awards of £6.2 million and ensured more than 55 years' worth of prison sentences were imposed on defendants found to be responsible for scams.

3.11 Alongside new forms of cybercrime, trading standards and other bodies are also seeing traditional areas of work moving towards a digital platform. A good example of this is counterfeiting of goods (DVDs, clothing, toys, foodstuffs, cosmetics and tobacco). According to the Intellectual Property Crime Report 2013/2014, social media has overtaken other auction websites as criminals' 'channel of choice' for counterfeit and piracy activity with figures indicating that 66 per cent of all UK adults have a social networking profile and 96 per cent of those a Facebook account.

3.12 Counterfeiting can range from the individual who copies DVDs on their home computer to large scale operations that import large quantities of counterfeit goods from abroad. Many of these goods come from countries that lack the rigorous safety checks that would usually be required to sells goods on the UK market. One major concern therefore is that counterfeit goods being sold through social media often have serious product safety issues and can pose majors threats to consumer safety.

3.13 It can be significantly more difficult to identify and prosecute an individual selling from an online platform than it is to investigate similar activity taking place in a local market. There has been a trend in recent years for more and more Social Networking Sites (SNS) traders to adopt closed privacy settings for both individual and joint accounts, alongside false user information which ensures that checks on subscriber details do not reveal their real location. For investigating officers it is

sometimes impossible to identify individuals utilising these types of closed accounts and this very often prevents enforcement action being taken by the investigating trading standards service.

3.14 All of these trends emphasise that in a fast-paced technological environment, with more criminal behaviour facilitated by or conducted over the internet, it is vital that all enforcement agencies, not just councils, have the right tools to tackle this.

3 **Are the new offences proposed in the draft Bill necessary? Are the suggested punishments appropriate?**

4.1 There are already a number of safeguards attached to councils' access to communications data, specifically the requirements that it is:

- authorised by a director, head of service or service manager (or someone who holds a higher position)
- managed through the National Anti-Fraud Network, and
- approved by a magistrates court.

4.1 Given these checks, it is unlikely that the proposed offence of unlawfully obtaining communications data could be incurred without deliberate intent to deceive, an action which might already be covered by existing offences such as misconduct in public office. The new offences of knowingly or recklessly acquiring communications data need to be very clearly defined within the draft Bill to distinguish between a genuine mistake and deliberate action. Furthermore it must be clear what the legal responsibilities and consequences are for inappropriate acquisitions submitted by an applicant, undertaken by a Single Point of Contact (SPOC) and authorised by a Designated Senior Officer (DSO).

4.2 Although we do not believe the new offences are strictly necessary, we recognise the intention to provide public assurance about proper use of the powers through the creation of a specific offence. We are confident that there will not be a need to invoke the offences proposed at section 8 of the Draft Bill in relation to council officers.

5 **How well does the current process under Mutual Legal Assistance Treaties (MLATs) work for the acquisition of communications data? What will be the effect of the extra-territorial application of the provisions on communications data in the draft Bill?**

5.1 Local authorities and the National Anti-Fraud Network have not sought any Mutual Legal Assistance Treaties as they do not apply to councils.

5.2 Some non-UK Communication Service Providers (CSPs) such who provide access to communications data on a voluntary basis through the Regulation of Investigatory Powers Act 2010 (RIPA) process. However, this area is sometimes sensitive, and a significant amount of work has gone into securing these arrangements to obtain access.

5.3 There are certain CSPs such as Google which will notify the subject of an enquiry due to the differing legal systems of the two countries. This can cause problems for investigations as tip-offs of this nature often lead to officers withdrawing requests for data as notifying the subject can be detrimental to ongoing investigations.

6 **Are the definitions of content and communications data (including the distinction between 'entities' and 'events') sufficiently clear and practical for the purposes of accessing such data?**

6.1 We support the introduction of new definitions of communications data (with entities and events data replacing subscriber, service use and traffic data). Under the current regime there has been confusion and legal uncertainty about the categorisation of certain types of data, and specifically whether they constitute subscriber or traffic data, with different CSPs sometimes taking different approaches. The updated legislation must resolve this confusion, or risk leading to further inconsistency among CSPs and early legal cases on this point.

6.2 It is therefore critical that there is clarity and consistency about the new definitions of communications data from the outset, and there are some areas where further explanation is essential. Government should provide specific guidance (in either the Bill or explanatory notes) as to the scope of entity and events data available to local authorities. This should clarify the extent of local authority powers with regards to how they can access and utilise this data to avoid confusion in the future.

7 **Does the draft Bill allow the appropriate organisations, and people within those organisations, access to communications data?**

7.1 The provisions in the draft Bill on access by councils and their officers mirror existing provisions on these issues. The LGA has not called for councils to have additional powers in this area, and therefore supports the approach proposed in the draft Bill.

7.2 For the reasons outlined above, we believe it is appropriate that local authorities should have the right to access communications data for the purpose of preventing or detecting crime.

7.3 We recognise the public assurance requirement for maintaining the existing arrangements under which council access to communications data must be authorised internally by a director, head of service or service manager or equivalent (or someone who holds a higher position).

7.4 However we have two concerns about the proposal. The first is that the requirement for operational independence of the DSO does not reflect that councils are already subject to internal member scrutiny processes, as well as to a fully independent authorisation process by magistrates. We therefore believe that the requirement for operational independence should not apply to local authorities.

7.5 A related concern is with senior officers who have a broad remit, as it can be challenging to take on a role which involves careful scrutiny of requests and awareness of a complex and ever-changing regulatory environment. For this reason, we welcome the proposal at section 62 of the draft Bill to allow 'collaboration agreements' such as the NAFN to take on the role of (among other things) DSO for other authorities. This provides the opportunity to ensure centres of excellence such as NAFN can provide critical functions on behalf of other authorities, as well as enabling flexibility within a changing local government landscape.

7.6 Further clarification is required as to the exact definition of a collaboration agreement that is certified by the Secretary of State, including that the certification required relates to the specific body itself (NAFN) rather than to each agreement it may reach with individual organsations (councils)

8 **Is the authorisation process for accessing communications data appropriate?**

8.1 Council access to communications data is currently subject to two specific safeguards which the draft Bill proposes to maintain.

8.2 The role of NAFN: Access to communications data is through NAFN, a local government shared service set up through two local authorities and now operating out of Tameside council. NAFN is independent of local authority investigations and imposes robust and comprehensive safeguards when receiving communications data requests. NAFN provides a guardian and gatekeeper role to ensure that all requests are legally compliant before authorisation by a Designated Person ahead of submission for judicial approval. All local authorities are required to submit their communication data requests to NAFN accredited SPOC's who are currently subject to annual inspection by the Interception of Communications Commissioner.

8.3 Going forward, NAFN is developing training and continuing professional development packages for local authorities and other non-law enforcement government departments (applicants, SPOCs, designated persons and senior responsible officers). In the longer term it may be possible for NAFN to offer formal accreditation through these packages.

8.4 In his recent review, the Independent Reviewer of Terrorism legislation praised the role and work of NAFN and suggested it could also be utilised by other public bodies accessing communications data.

8.5 Approval from a magistrate's court: The requirement for councils to seek judicial approval of access to communications data provides assurance for the public that this power is being used appropriately. The fact that only 19 out of 6,000 requests to magistrates have been refused demonstrates that this is the case.

8.6 However, in practice the process of seeking judicial approval can be slow and inefficient. Some councils have reported it can take as much as 5 hours of officer

time to gain approval because of the need to attend court to do so. We are aware that the process acts as a deterrent to councils seeking access to communications data when there is a legitimate basis for them to do so.

8.7 It is vital that the court system works effectively to enable councils to seek and be granted online judicial approval, which would not weaken this safeguard but would make it significantly more efficient.

8.8 It would be beneficial for all requests for judicial approval to be made by NAFN on behalf of individual local authorities. We understand that there would be initial administrative and resource challenges for local courts close to NAFN's host authority in Tameside (as well as issues in relation to Scotland and possibly Northern Ireland in the future). However, by providing a centre of magistrates' expertise, this would ensure the safeguard operates on a robust and consistent basis in future.

9 **What are the advantages and disadvantages of the proposed creation of a single Judicial Commission to oversee the use of investigatory powers?**

9.1 The creation of a single body to oversee the use of investigatory powers will be beneficial in terms of ensuring a consistent approach to the interpretation of key issues. The different bodies with oversight of this area have in the past occasionally reached different interpretations of issues relevant to local authorities (for example, the DSO role): a single, consistent view will be helpful.

Annex - Case studies showing how councils use communications data

Set our below are a number of case studies providing examples of how local authorities have used communications data to identify criminal activity, and bring prosecutions against the perpetrators.

Protecting the vulnerable

Operation Violet
Operation Violet led to the jailing of five members of a family for conning elderly people out of hard earned savings. The gang preyed on at least 81 victims who came from Yorkshire, Derbyshire, Staffordshire, Nottinghamshire and as far south as Essex. Trading Standards were only able to identify the gang and connect them with their victims through access to communications data.

The court heard they conned or tried to defraud them of £175,645, according to the charge sheet. However, the prosecution accepted the real number of victims and the scale of their losses was incalculable. A confiscation hearing under the Proceeds of Crime Act involved a claim of nearly £1 million.

Gang leader David Price Snr, 42, was given a sentence of seven years and eight months. His sons Abraham, 20, and David Jnr, 19, were sent to Young Offenders' Institutions for three years and eight months and three years and four months respectively. Angelina Price, 40, the leader's wife, was jailed for 16 months and his brother Shane, 41, was sentenced to three years and four months. Family associate James Cunningham, 26, from Castleford, West Yorkshire, was jailed for five years and four months.

Operation Crossbill
The initial subscriber check assisted in identifying the main perpetrator of a crime of fraud committed against an elderly vulnerable male. The subsequent itemised billing for the relevant period demonstrated calls were made to the victim from the perpetrators phone on the time and dates alleged by the victim and corroborates his story. The subscriber check requested thereafter was to confirm the telephone was being used by the money launderer. This demonstrated calls to the victim and calls to the perpetrator at the relevant times and thus again corroborated the victims story.

The telecoms data identified an offender and supported the allegation made by the victim. The total monetary value for this investigation was £8,100. Subsequent arrests and searches resulted in evidence of two further crimes.

Current case: Operation Travalger
Operation Travalgar is a long-running fraud investigation into the activities of a number of suspects who defraud older consumers by means of cold calling, and then signing the victims up to roofing work which is unnecessary and involves the application of paint. False claims are made regarding the properties of this paint, and sums in the low thousands of pounds are generally extracted in return for the work. As the result of the particular subscriber check and itemised billing, a suspect was identified and two further individuals were arrested and

are bailed until mid-January 2016 on suspicion of fraud. The data recovered from the further suspect's phones has yielded many more recent victims. It is anticipated that the suspects will be charged with fraud by false representation in January 2016.

It was solely as the result of the communications data that the further suspects and victims were identified. This tool is central and vital to the work that the regional investigation teams within Trading Standards do. It is used sparingly and proportionately; without access to this data it simply would not be possible to detect the criminals the teams are dealing with.

Tackling organised crime

Operation Magpie – Cambridgeshire County Council
Operation Magpie concerned an investigation into an organised crime group who defrauded elderly and vulnerable people. The criminals exploited their victims to the extent that one person was evicted from their home, and they also laundered cheques to the value of £700,000.

The ringleader of the gang received a prison sentence of 7 years with two co-conspirators receiving sentences of 5 years each. 16 other offenders were also convicted of money laundering offences serving prison sentences of up to 30 months.

Malcolm Taylor from Trading Standards at Cambridgeshire County Council said "Without access to communications data, we would not have been in a position to connect the conspirators and detect the level of criminality that extended to over 100 vulnerable and elderly victims, some of whom have since died".

Operation Troy – Suffolk County Council
Operation Troy was a long running advanced fee fraud case that was investigated and prosecuted by Suffolk's trading standards service. The fraud operated between 2007 and 2010, involved at least £7.5 million of consumer detriment affecting well over 16,000 consumers and involved two distinct frauds;

- An escort/companion fraud in which consumers were offered guaranteed work as escorts and companions in return for a registration fee, however no work was subsequently provided.
- A debt elimination fraud in which consumers paid an advanced fee to receive a debt elimination service but little or no service was ever provided.

The fraud was complex and well organised, operating from call centres in Spain. UK customers made contact with the call centres using free phone numbers that appeared to be UK based after viewing various escort websites offering work. During calls with escort agency staff, false promises would be made regarding the immediate availability of work and potential earnings available. Many consumers complained of similar experiences and provided similar accounts of last minute cancelled work appointments after they had paid their fees.

The escort websites and telephone numbers changed frequently to confuse consumers and make it difficult for enforcement bodies to track the source of the fraud. By using RIPA powers and obtaining communication data for the telephone numbers used for the fraud, the following links were established:

- The multiple telephone numbers were owned and operated by only two individuals. One of those individuals, who held the majority of the numbers, had been identified as being involved in operating multiple UK bank accounts used for money laundering aspects of the fraud and the creation of shell companies.
- All the UK free phone numbers were being redirected to Spanish based numbers that were linked to a small number of call centres operating from the Malaga area of Spain. These call centres were all owned by one man who was known to have a previous history of fraudulent trading.
- The link provided by this communication data provided evidence that what appeared outwardly to be over 12 different separate escort websites/agencies were in fact all one fraud perpetrated by one set of linked individuals.

In June 2012 European Arrests warrants were applied for in respect of Antoni Muldoon, the man at the helm of the fraud, and two other members of the gang, Geraldine French and Bradley Rogers. All three were returned to the UK. Following extradition in September 2012 Muldoon pleaded guilty to conspiracy to defraud at Ipswich Crown Court.

Following Muldoon's plea, and after a series of trials at Ipswich Crown Court including a ten week trial involving five of the defendants that concluded in June 2013, seven further members of the gang were found guilty of offences including conspiracy to defraud and money laundering offences. The sentences handed down totalled 36 years overall, with Muldoon receiving 7.5 years for his role and Mark Bell of Ipswich, Muldoon's right hand man in the UK, receiving 6.5 years.

Confiscation proceedings followed the sentencing and over £1m was awarded in confiscation and costs, which Suffolk Trading Standards has used to repay victims of the fraud. The confiscation amount for Antoni Muldoon, who benefited to the largest extent from these crimes, was £750,000. In July 2014 four of the defendants appealed their convictions and sentences at the Court of Appeal in London and in front of three sitting High Court Judges all appeals were turned down.

Steve Greenfield, Suffolk's Head of Trading Standards and Community Safety commented that 'RIPA powers were essential to the successful outcome of this case.'

Protecting people from dangerous goods

Current case: Clocked Vehicles
This particular application related to an operation into the sale of clocked cars with fraudulent service histories by Polish nationals in Worcestershire. At the time of the application 40 vehicles had been fraudulently sold in this way to consumers nationally. Criminal offences are being investigated under the Fraud Act 2006 and the Consumer

Protection from Unfair Trading Regulations 2008. The offenders were using multiple Pay as you Go phones and were meeting consumers in the street. It was not known where the offenders were living and open source information did not reveal these details.

As a result of the application one of the mobile numbers used was found to be registered to a known suspect who had taken payment for a car. An address was also obtained from this mobile phone data. Evidence to corroborate the identity of those living at the address was then obtained which resulted in an entry warrant being executed by Worcestershire Trading Standards and West Mercia Police. Two suspects were arrested and are currently on bail. Evidence obtained from the house included multiple mobile phones, blank service history books and fraudulent service stamps used to create false service histories.

The investigation is ongoing. Without this communications data the offenders address would not have been identified and vital evidence would not have been obtained. It is possible the offenders would not have been caught. The current total value of the fraud is £115, 000. The total mileage deducted from vehicle odometers is almost 1.4 million miles.

Fraudulent car trader
A car trader was convicted of multiple offences contrary to the Fraud Act 2006 in relation to the sale of misdescribed and clocked cars. Vehicles were purchased at auction with higher mileage and advertised online via AutoTrader. The trader claimed a third party was responsible and he simply allowed the third party to use his account at auction to obtain vehicles more easily. However, SIM cards found in possession of the car trader were confirmed, using communications data, as being associated with unregistered PAYG telephone numbers used in adverts for vehicles. During the course of the investigation, the trader sold his house and moved location; a second set of communications data (forwarding address details from Royal Mail) helped to locate him for the purposes of arrest, entry warrants and interview. The penalty was 12 months imprisonment and a Proceeds Of Crime Act confiscation order in excess of £58,000.

Protecting businesses

Counterfeit goods case study 1
Two internet traders based in Slough were selling counterfeit trainers on e-bay for £35.00. The only intelligence the trading standards service had was the e-mail address and mobile phone numbers that the complainants used to make the purchase. The actual retail price of these trainers was £135 a pair. By obtaining the data from the mobile phones and the I.P address the council were able to pinpoint the address being used by the perpetrators. A test purchase had been made prior to a warrant being sought. A sting operation resulted in a seizure of trainers with a street value of £325,000 and both offenders received a custodial sentence. Without communications data, this would not have been possible.

Counterfeit goods case study 2
Officers seized some potentially counterfeit mirrors from a shop. By the time the mirrors were confirmed as being counterfeit the trader had disappeared after failing to attend for interview. The contact details he provided proved to be false. However, officers obtained a mobile number for the trader and the subscriber details identified his home address in

Swansea. This enabled officers to contact him. He subsequently pleaded guilty to 3 offences under the Trade Marks Act. Without the access to the communications data officers would not have been able to find the new address to which he had moved and so the investigation would not have been able to proceed.

Protecting taxpayers

Barnet council – rent deposit scheme fraud
A man and woman were jailed following a Barnet Council investigation to crack a highly organised plot to obtain fraudulent payments from the authority by using a complex web of false identities to open a string of bank accounts which were then activated to receive thousands of pounds in fraudulent rent deposit scheme payments. The rent deposit scheme is used by the council to provide people in need of housing with initial financial support to help secure a tenancy for private rented accommodation.

The investigation by the council's Corporate Anti-Fraud Team (CAFT) was launched after uncovering irregularities with a number of rent deposit payments. Investigators went on to identify 41 fraudulent payments worth £132,629 which had been paid to different bank accounts. During the course of the investigation a further 12 fraudulent payments worth more than £31,600 were intercepted and blocked by CAFT.

CAFT worked with NAFN to obtain mobile phone records, under the Regulation of Investigatory Powers Act, which provided significant evidence to show that the accused were in regular contact on the days when substantial withdrawals and deposits were made. The powers also enabled the investigators to identify the real owners of the false identities by obtaining the mobile phone service providers records which identified names and addresses where these suspects could be found. The legislation also allowed information of redirected post from credit card companies, banks and online purchase deliveries which also assisted in tracing addresses that the suspects used which were then the subjects of police / CAFT raids. Without access to this information the investigation would not have proceeded to a useful outcome.

Landfill tax fraud
A council was alerted to a skip hire company who were disposing of waste in an unauthorised manner, including avoiding payment of landfill tax estimated at £1.3 million. Enquiries made by the council identified three suspects but there was no evidence to link them to the offences. Subscriber and itemised billing data provided by NAFN proved that there were regular communications between the individuals during periods in question. Without this information, it would have been impossible to pursue a prosecution.

Tenancy fraud
Family members and care homes called the council to advise that a council tenant had moved out and the agency worker then took the keys back and pretended to be a private sector landlord. The council has now identified 13 properties that were illegally sublet by an agency worker using adverts on Gumtree. The loss to the council concerned is estimated at up to £819,000; the cost of housing tenants in the private sector rather than in the Council's

housing stock. This is believed to be the biggest example of housing tenancy fraud investigated.

Communications data helped to reveal the extent of the fraud, identified the whereabouts of the fraudster, provided details of all the tenants (many of who are now acting as witnesses) and gave important information about other parties connected to the crimes.

Identifying Associates

In August 2009 a container came into Tilbury Dock from Pakistan to be forwarded to a consignee, being a company in Rhondda Cynon Taff run by PL. Inside the container HMRC staff found counterfeit garments and beds.

Council officers obtained itemised billing for PL's phones in October 2009 and analysis identified various other associates who were working with PL, including a Mr and Mrs SI in Essex. Further subscriber checks were carried out in February 2010 to identify parties who had not been identified by other means. After another delivery of 528 jeans was intercepted on behalf of the council by HMRC at Heathrow Airport in March 2010, officers executed warrants at various premises associated with PL and Mr and Mrs SI. Various computers, paperwork, labels and counterfeit garments were seized, including 40 counterfeit jeans and 5000 labels from the Mr and Mrs SI.

Subsequent examination of the records on these computers and information from the billing checks and other enquiries led to further warrants being executed by council officers in July 2010 at premises in Newport, Leicester, Redbridge and Essex. Significant evidence was obtained and as a result PL and various other associates are under investigation for offences of conspiracy to commit Trade Marks Act offences.

18 December 2015

Annie Machon—written evidence (IPB0064)

1. My name is Annie Machon and I worked as an intelligence officer for the UK's domestic Security Service, commonly referred to as MI5, from early 1991 until late 1996. I resigned to help my partner at the time, fellow intelligence officer David Shayler, expose a number of instances of crime and incompetence we had witnessed during our time in the service.

2. I note that the draft IP Bill repeatedly emphasises the importance of democratic and judicial oversight of the various categories of intrusive intelligence gathering by establishing an Investigatory Powers Commissioner as well as supporting Judicial Commissioners. However, I am concerned about the real and meaningful application of this oversight.

3. While in the Service in the 1990s we were governed by the terms of the Interception of Communications Act 1985 (IOCA), the precursor to RIPA, which provided for a similar system of applications for a warrant and ministerial oversight.

4. I would like to submit evidence that the system did not work and could be manipulated from the inside.

5. I am aware of at least two instances of this during my time in the service, which were cleared for publication by MI5 in my 2005 book about the Shayler case, “Spies Lies, and Whistleblowers”, so my discussing them now is not in breach of the Official Secrets Act. I would be happy to provide further evidence, either written or in person, about these abuses.

6. My concern about this draft Bill is that while the oversight provisions seem to be strengthened, with approval necessary from both the Secretary of State and a Judicial Commissioner, the interior process of application for warrants will still remain opaque and open to manipulation within the intelligence agencies.

7. The application process for a warrant governing interception or interference involved a case being made in writing by the intelligence officer in charge of an investigation. This then went through four layers of management, with all the usual redactions and finessing, before a final summary was drafted by H Branch, signed by the DDG, and then dispatched to the Secretary of State. So the minister was only ever presented with was a summary of a summary of a summary of a summary of the original intelligence case.

8. Additionally, the original intelligence case could be erroneous and misleading. The process of writing the warrant application was merely a tick box exercise, and officers would routinely note that such intelligence could only be obtained by such intrusive methods, rather than exploring all open source options first. The revalidation process could be even more cavalier.

9. When problems with this system were voiced, officers were told to not rock the boat and just follow orders. During the annual visit by the Intelligence Intercept Commissioner, those with concerns were banned from meeting him.

10. Thus I have concerns about the realistic power of the oversight provisions written into this Bill and would urge an additional provision. This would establish an effective channel whereby officers with concerns can give evidence directly and in confidence to the Investigatory Powers Commissioner in the expectation that a proper investigation will be conducted and with no repercussions to their careers inside the agencies. Here is a link to a short video I did for Oxford University three years ago outlining these proposals:

11. This, in my view, would be a win-win scenario for all concerned. The agencies would have a chance to improve their work practices, learn from mistakes, and better protect national security, as well as avoiding the scandal and embarrassment of any future whistleblowing scandals; the officers with ethical concerns would not be placed in the invidious position of either becoming complicit in potentially illegal acts by "just following orders" or risking the loss of their careers and liberty by going public about their concerns.

12. I would also like to raise the proportionality issue. It strikes me that bulk intercept must surely be disproportionate within a functioning and free democracy, and indeed can actually harm national security. Why? Because the useful, indeed crucial, intelligence on targets and their associates is lost in the tsunami of available information. Indeed this seems to have been the conclusion of every inquiry about the recent spate of "lone wolf" and ISIS-inspired attacks across the West – the targets were all vaguely known to the authorities but resources were spread too thinly.

13. In fact all that bulk collection seems to provide is confirmation after the fact of a suspect's involvement in a specific incident, which is surely specifically police evidential work. Yet the justification for the invasive intercept and interference measures laid out in the Bill itself is to gather vital information ahead of an attack in order to prevent it – the very definition of intelligence. How is this possible if the sheer scale of bulk collection drowns out the vital nuggets of intelligence?

14. Finally, I would like to raise the point that the phrase "national security" has never been defined for legal purposes in the UK. Surely this should be the very first step necessary before formulating the proposed IP Bill? Until we have such a legal definition, how can we formulate new and intrusive laws in the name of protecting an undefined and nebulous concept, and how can we judge that the new law will thereby be proportionate within a democracy?

20 December 2015

Rt Hon Theresa May MP—supplementary written evidence (IPB0165)

The draft Investigatory Powers Bill: Following up to 13 December evidence session.

Thank you for the opportunity to appear as a witness before your Committee last week to inform your pre-legislative scrutiny of the draft Investigatory Powers Bill. As I said at the beginning of the session, I am very grateful to you and the other members of the Committee for your thorough and comprehensive scrutiny of the draft Bill and look forward to receiving your report in due course.

During the evidence session, I undertook to follow up in writing on a number of areas and this letter provides the additional detail I committed to provide. The case for the bulk powers included in the Bill is attached at the Annex, separated by power.

I would also like to take this opportunity to emphasise a point from my evidence last week on the merits of including a sunset provision in the Bill. Such measures are often used in emergency legislation where either the legislation has been brought in to address a specific short term challenge or where Parliament was given limited time to consider the legislation. Neither is the case here – this legislation is intended to reform and modernise the investigatory powers available to the security and intelligence agencies, law enforcement and other public authorities and used in support of their core activities.

There are practical issues with introducing artificial deadlines. Many of the provisions in the Bill, such as the data retention obligations, require a considerable investment of time and effort from communications service providers to put in place the necessary infrastructure. The systems which need to be developed are complex and can take over 12 months to design and implement.

Inserting a sunset clause – of whatever period – would create uncertainty among communications service providers. They may be reticent to invest the same time and effort as they historically have done. The solutions that they implement may as a result fail to deliver maximum operational benefit, efficiency or value for money.

In drafting the Bill we have sought to create legislation that will stand the test of time, but I recognise that there will come a point when it will need to be revisited in whole or in part. However, technology does not advance according to a set schedule, and a sunset clause would set an arbitrary deadline for review.

I therefore have considerable concerns about the potential for such a provision to stifle innovation, limit operational effectiveness and increase cost. There will of course be considerable Parliamentary interest in understanding the benefit that internet connection records in particular deliver over the coming years. That is why the work of the Investigatory Powers Commissioner — whose reports will be presented to Parliament — will be vital in providing assurance and considering whether and when any of the provisions in the Bill should be revisited.

Specific points of follow up - How are intelligence sharing arrangements with overseas partners governed? If not on the face of the bill, what safeguards are in place to ensure protections cannot be circumvented? What law applies?

The new legislation will make clear the safeguards that apply when intercepted material or data is disclosed to other countries. Safeguards for sharing intercepted material will be provided in Codes of Practice made under the new legislation. These safeguards will explain the processes that will be followed before an interception request could be made to another country and how any material received as a result would be handled, and makes clear that the agencies cannot get around the protections afforded by the Bill by asking an international partner to undertake interception on our behalf.

Robust and detailed Codes of Practice on investigatory powers are in place under current legislation which make information publically available about the safeguards which govern the sharing of intercepted material between our security and law enforcement agencies and our international partners. The provisions in the Codes bring greater transparency to the robust processes that the security and intelligence agencies adhere to when targeting terrorists', criminals' and hostile states' communications to prevent terrorism, curb organised crime and identify and stop others who seek to harm us and our country. This information will be replicated in Codes of Practice issued under the Bill.

More broadly, it remains the case of course that the agencies are subject to the general provisions in the Security Service Act and Intelligence Services Act that set out their functions and the requirement that they disclose information only where it is necessary and proportionate to do so in carrying out those functions. The Foreign Secretary reviews all international intelligence sharing arrangements on a six-monthly basis through a formal submission. This is an over-arching review and covers all intelligence relationships between the security and intelligence agencies and overseas agencies and is currently overseen by the Intelligence Services Commissioner.

Can Data Retention Notices be disclosed under the Freedom of Information Act?

It has long been the practice of Governments not to disclose the existence of data retention notices. Disclosing the existence of a notice would risk undermining national security and the prevention and detection of crime. For example, criminals might start to use the services of companies that are not subject to a notice. The commercial interests of that company could be prejudiced if the Government made the fact of a notice public and significant numbers of customers transferred their business to companies who are not subject to a notice.

This approach has been upheld by the Information Commissioner when he has considered appeals to Freedom of Information requests on this point. The existing data retention code of practice makes clear that the Home Office does not disclose this information. Communications service providers, as private entities, are not bound by the requirements of the Freedom of Information Act. The draft IP Bill makes clear that CSPs must not disclose the existence of a notice.

For the first time, the Bill will allow CSPs affected by a notice to seek a review of that notice. As part of the review the Secretary of State must seek the view of the Investigatory Powers Commissioner on the proportionality of the notice. Additionally the IPC will now have oversight of the retention provisions in the Bill and these provisions are now within scope of the Investigatory Powers Tribunal's functions.

The issuing of Data Retention Notices is taken very seriously by the Government and, as the Bill states, CSPs can only be required to retain relevant communications data if the Secretary of State considers it to be necessary and proportionate. Although the notices will not be made public we consider that the oversight arrangements will provide significant reassurance as to the implementation of these powers.

Internet Connection Records (ICRs)

The Committee requested further information on the utility of ICRs and feasibility and costs of implementing ICR retention. Law enforcement may seek ICRs for a number of reasons consistent with the three purposes for which ICRs can be accessed under the Bill. These include:

- To understand who has accessed a communications service/site or server hosting child exploitation images at a specific time/date;
- To establish who may be running network scans against a specific piece of critical nation infrastructure;
- To identify if a subject of interest used an online communication service;
- If a person is missing or has been killed to establish if they were in contact with anyone before their disappearance or death;
- Where an individual of interest is known to be communicating online but it is not known how;
- To identify which file sharing sites a person has uploaded illegal images to;
- To identify contacts of a suspect following the seizing of a communication device;
- Where a person is known to have accessed a site containing child exploitation images, to establish whether they have accessed other sites containing similar material or to establish whether they have uploaded this material to another website or server;
- To identify if a person suspected of owning illegal weapons has been accessing illegal online market places;

Some witnesses have made the point that in some cases all an ICR will show is that a person is permanently connected to a certain social media application, and have therefore argued that this undermines the utility of ICRs. The examples listed above includes seeking to establish whether a missing or murdered person was in contact with anyone before their death. An ICR itself may not, as you have heard, tell an investigator that an individual has been in contact with another individual. But what it could tell an investigator is the communication service, or services, that a person has been using. That in turn would enable subsequent requests to be made to those providers. Without ICRs, it would not even be

possible to make these subsequent requests as the identity of the providers is unlikely to be known.

As I have set out in my previous written submission, the components which make up an ICR may depend on how a communications service provider configures and runs its network. Where a requirement to retain internet connection records is identified we will work closely with the communications service provider concerned to determine the exact data types that they specifically will be required to retain, rather than requiring them to retain all the data types that meet the internet connection records definition – something that may not be feasible for all CSPs.

In terms of the costs provided in the impact assessment, these are based on the development and implementation of internet connection records solutions prioritised by operational need. Not all UK communication service providers will be required to retain internet connection records.

Costs to implement internet connection records are an initial estimation based on feasibility analysis undertaken by the Home Office in consultation with communications service providers and the anticipated approach to implementation.

The estimated costs for implementing the internet connection records solutions were shared with UK communications service providers during the summer of 2015. At this time CSPs were asked for their assessment of the proposed costs and for the implications of implementing ICR solutions. The responses provided by CSPs were used to revise the cost estimates and assumptions that informed the impact assessment. The costs in the impact assessment have been profiled across a ten year period to reflect a realistic deployment schedule and have been subject to standard government financial treatments.

The impact assessments produced for the Bill, of course, assess the economic impact of new policy. They do not include the current costs of existing legislation. For example existing legislation (the Counter-Terrorism and Security Act 2015) allows for the retention of IP address resolution data, the economic costs of which were assessed to be £9.6million per annum. The costs in the impact assessment only relate to the retention of the additional data.

These costs will be refined as we move into more detailed definition discussions on individual CSP specific implementations.

Supplementary questions requested by the Joint Committee

In addition to the specific points of follow-up above, I understand that the Committee had a further three questions to ask which time did not permit. We have received these questions from the Committee clerks to which we provide written responses below.

Some witnesses have suggested simply removing Cl. 19 (2) and the reference to judicial review principles. What would the impact be?

I firmly believe that judicial review principles are the correct test to be applied by the Judicial Commissioners. The reason for this, which I hope I made clear in my evidence to the Committee, is that judicial review principles provide a flexible test that allows for differing degrees of intensity of scrutiny that can be adapted and applied as appropriate in the circumstances and the impact of the decision on the individual concerned. This is the point that Lord Pannick made in his article of 12 November 2015.

The Judicial Commissioners who will be scrutinising the warrant authorisations will be experienced senior judges, who are well versed in judicial review and how to apply the principles to an Executive decision. As the three existing oversight Commissioners, all themselves very experienced members of the Judiciary, made clear to the Committee in their evidence, judicial review principles is the right test to be applied. Therefore the inclusion of this reference in the bill provides clarity about the process and the test being applied that will be lacking if it is removed.

Is there any update on the status of Sir Nigel Sheinwald's recommendation regarding international arrangements with overseas communications service providers?

All of the independent reviews into investigatory powers recognised the issue of longer-term international arrangements with communications service providers. David Anderson recommended that extraterritorial application should continue to be asserted in relation to UK warrants and authorisations, and that the UK develop and negotiate an international framework among like- minded democratic nations for accessing data across jurisdictions. We have continued to engage in preliminary discussions with international partners on how such an agreement might operate in principle, based on strong, human rights-compliant domestic regulatory frameworks. In the discussions I have held, there is a consensus about the broad principles behind an agreement, but we are not yet at the stage of any formal negotiations.

Such an agreement would be good for business who require greater certainty in the face of conflicts of laws; good for the public, because it would increase levels of transparency and oversight, while also ensuring they are protected from key threats; and good for the internet, because it would avoid the challenges posed by the data localisation and the "balkanisation" of the web. Longer term, I am keen to ensure wider international cooperation among all partners who share transparent, accountable human rights compliant arrangements. Of course our primary objective is to ensure law enforcement and the security and intelligence agencies remain able to access the communications of serious criminals, terrorists and hostile foreign actors who pose a threat to the public, whilst also raising standards of oversight and transparency and finding multi-stakeholder solutions to today's global problems.

Why is the right of appeal from the Investigatory Powers Tribunal limited to cases where (a) the appeal would raise an important point of principle or (b) there is another compelling reason for granting leave? [Clause 180]

This draft Bill creates, for the first time, a domestic route of appeal from the Investigatory Powers Tribunal (IPT). This will allow more complainants the chance to have their case heard

by another domestic court. However, I believe that it is right that this appeal right is limited. This is because a significant number of claims submitted to the IPT each year are entirely without merit. Of the 205 cases that were considered by the IPT in 2013 (the last published figures):

- 53% were deemed to be frivolous or vexatious
- 31% were given a "no determination"
- 10% were out of the jurisdiction of the IPT; and the remaining
- 6% were out of time

Therefore, whilst creating an appeal route is important, not having any limits on that route would mean a considerable amount of tax-payer money and agency time and resource would be wasted on continuing to defend cases that have no grounding in fact or merit in law. I believe that allowing a person to appeal on a point of principle, or where there IPT considers there are compelling circumstances to allow an appeal, is the right threshold that will still allow important cases that are worthy of further Judicial scrutiny to progress to the Court of Appeal. This approach is consistent with available appeal routes found in other contexts, such as judicial review challenges from an Upper Tribunal, reflecting that restricting the scope of appeals is necessary to ensure only the most compelling appeals progress to the highest courts. I hope the additional information clarifies these points for the Committee but if my officials can be of any further help then please do not hesitate to contact them.

ANNEX – THE CASE FOR BULK CAPABILITIES

BULK INTERCEPTION

Bulk interception is a vital tool designed to obtain foreign-focused intelligence and identify individuals, groups and organisations overseas that pose a threat to the UK. Bulk interception is crucial because the security and intelligence agencies frequently have only small fragments of intelligence or early unformed leads about people overseas who pose a threat to the UK. Equally, terrorists, criminals and hostile foreign intelligence services are increasingly sophisticated at evading detection by traditional means. Access to large volumes of data enables the intelligence agencies to piece together communications and identify patterns of behaviour.

This is important to: establish links between known subjects of interest; search for traces of activity by individuals who may not yet be known to the agencies but who surface in the course of an investigation; or to identify potential threats and patterns of activity that might indicate a national security concern. Just as importantly, due to the nature of the global internet, the route a particular communication will travel is hugely unpredictable. Access to large volumes of data is essential to enable communications relating to subjects of interest to be identified and subsequently pieced together in the course of an investigation.

Current Position

Bulk interception is provided for under section 8(4) of the Regulation of Investigatory Powers Act 2000 (RIPA). Under the current regime, a warrant issued by the Secretary of State must consider the necessity and proportionality of the proposed interception and whether the information collected through interception could reasonably be obtained by other means. An interception warrant issued under section 8(4) of RIPA must be accompanied at the time of its issue by a certificate, also issued by the Secretary of State, certifying a description of intercepted material the examination of which is considered necessary.

The conduct authorised by an interception warrant issued under 8(4) must be confined to the interception of "external communications", defined as those which are sent or received outside the British Islands. Conduct authorised under a section 8(4) warrant may sometimes result in the incidental interception of communications that were both sent and received in the British Islands; RIPA permits this only if it is necessary to intercept the external communications that are the target of the warrant. Before material intercepted under a section 8(4) warrant may be examined, it is subject to a further consideration of necessity and proportionality. If an analyst wishes to select for examination the content of the communications of an individual known to be located in the British Islands, he or she must apply to the Secretary of State for an authorisation under section 16(3) of RIPA. This process is similar to the application for a warrant under section 8(1).

Safeguards in the Bill

The IP Bill will maintain the security and intelligence agencies' capabilities to undertake bulk interception without introducing any new powers. As is the case with an interception

warrant under 8(4) of RIPA, a bulk interception warrant will be foreign-focused and its main purpose must be limited to the interception of "overseas-related" communications. These are defined as those communications sent or received by individuals outside the UK.

The Bill will introduce new safeguards in relation to bulk interception warrants. Bulk interception warrants, as well as targeted interception warrants, will continue to be issued by the Secretary of State but will now also need to be approved by a Judicial Commissioner before they can be issued. This will provide a new "double-lock" authorisation procedure. A bulk interception warrant will need to set out specified "Operational Purposes". No intercepted material or data may be examined unless doing so is necessary for one or more of the operational purposes. Those specific purposes must be approved as being necessary by a Secretary of State and a Judicial Commissioner.

As currently, a bulk interception warrant may, incidentally, intercept the communications to or from an individual in the UK, due to the global nature of modern online communications. The content of communications of persons known to be in the UK may only be selected for examination under the Bill when a targeted examination warrant under Part 2 of the Bill has been obtained. The process for the authorisation of a targeted examination warrant will be the same as that for a targeted interception warrant. It will need to be issued by the Secretary of State and approved by a Judicial Commissioner before being issued. Only the security and intelligence agencies will be able to apply for a bulk interception warrant and only in relation to three statutory purposes: in the interests of national security, for the prevention or detection of serious crime and in the interests of the economic well-being of the UK, where there is also a direct link to national security. National security must always be one of the statutory purposes for which a bulk interception warrant is authorised.

The Value of Bulk Interception

Attack planning in Europe

In 2014, GCHQ analysis of bulk data uncovered a previously unknown individual in contact with a Daesh-affiliated extremist in Syria who was suspected of involvement in Western attack planning. Despite attempts by the individual to hide his activity, GCHQ was able to use bulk data to identify that he had travelled to a European country and separate intelligence suggested he was progressing with attack planning. The information was passed to authorities in that country, enabling the successful disruption of the attack planning. During the disruption several home-made IEDs were found.

Access to extreme indecent images

Using bulk data to spot patterns of behaviour demonstrated by paedophiles, in 2013 GCHQ identified a UK national using sites containing images of child sexual exploitation that required a payment to access the most extreme indecent images. This individual had previously held a position that provided him with access to children (and was on the Violent and Sexual Offenders register). He was sentenced to 3 years imprisonment and made subject to a Sexual Offenders Harm Order for life.

Annex 9 of David Anderson's report "A Question of Trust" also contains helpful examples of the importance of bulk interception capabilities.

BULK COMMUNICATIONS DATA

Where a security and intelligence agency has only a fragment of intelligence about a threat or an individual, communications data obtained in bulk may be the only way of identifying a subject of interest.

Fast and secure access to large volumes of data is essential to the security and intelligence agencies to progress their investigations. It enables the identification of communications data that relates to subjects of interest and to subsequently piece together the links between them. Carefully directed searches of large volumes of data also allow the security and intelligence agencies to identify patterns of activity that significantly narrows down the areas for investigation and allows them to prioritise intelligence leads.

Identifying the links between individuals or groups can also help the security and intelligence agencies to direct where they might request a warrant for more intrusive acquisition of data, such as interception. It allows them to search for traces of activity by previously unknown subjects of interest who surface in the course of an investigation in order to identify them.

In many cases bulk communications data provides the only investigative lead that the agencies have to be able to work with. Communications data has played an important part in every Mi5 investigation over the last decade and communications data in bulk has been used by the SIA to deal with the most serious threats facing the UK.

Current Position

There is an existing power for the Secretary of State to issue directions to communications service providers under section 94 of the Telecommunications Act 1984 which has enabled the security and intelligence agencies to obtain communications data in bulk.

The security and intelligence agencies' use of the section 94 power has been approved by successive governments and Secretaries of State. Directions issued in relation to bulk CD are reviewed every 6 months. The Prime Minister made a statement in March 2015 that the Interception of Communications Commissioner provided oversight of the use of section 94.

Safeguards in the Bill

Under the Bill bulk acquisition warrants will be issued by the Secretary of State but will now also need to be approved by a Judicial Commissioner before they can be issued. This will provide a new "double-lock" authorisation procedure.

A bulk acquisition warrant will need to set out specified "Operational Purposes" for which any of the data that has been collected can be examined. Those specific purposes will be approved by a Secretary of State and a Judicial Commissioner and might include, for

example, “attack planning by Daesh in Syria against the UK”. No data may be examined except for those purposes.

Only the security and intelligence agencies will be able to apply for a bulk CD acquisition warrant and only in relation to three statutory purposes: in the interest of national security, for the prevention and detection of serious crime and in the interest of the economic well-being of the UK, where there is also a direct link to national security. National security must always be one of the statutory purposes for which a bulk acquisition warrant is authorised.

Bulk acquisition warrants must be served on a communications service provider. The power cannot be used by an intelligence agency to acquire communications data from a telecommunication system themselves.

The Value of Bulk Communications Data

Access to domestic bulk communications data has enabled MI5 to thwart a number of attacks here in the UK.

Counter Terrorism
In 2006, a group of terrorists were planning to bring down multiple commercial aircraft using improvised explosive devices, in an attack reminiscent of the Lockerbie bombing. If carried out successfully, it would have been the largest terrorist attack on UK citizens ever, with a death toll similar to the 9/11 attacks.

Using bulk communications data, the intelligence agencies were able both to identify the plotters and develop greater understanding of their network, and to ensure the police were in a position to arrest them before the attack could be carried out. These individuals were subsequently tried and convicted for their part in the conspiracy.

Furthermore, the security and intelligence agencies’ ability to access domestic communications data in bulk provided them with the means to track a connected plot and identify all involved very quickly. This ensured measures could be put in place to prevent further attacks being attempted. Without access to this data, much more time consuming individual analyses of communications data would have been necessary to identify this cell, which would have resulted in the intrusion into the privacy of a significant number of innocent people.

Counter Terrorism
In 2010, a group of terrorists were plotting to blow up several symbolic locations in the UK, including the London Stock Exchange. Following an intensive investigation, in which analysis of bulk communications data played a key role, particularly given considerable geographical separation of different parts of the network, the group were all identified and their plot uncovered. The security and intelligence agencies were able to work with police to disrupt them in time and the group were charged with terrorism offences, including conspiracy to cause an explosion. All entered a guilty plea in light of the weight of evidence against them and were sentenced to prison terms.

Counter Terrorism
Following a failed attack in London in 2007, the security and intelligence agencies were able to confirm that the perpetrators were the same as a group who had carried out another attack shortly afterwards. This was achieved in a matter of hours through the analysis of bulk communications data, and was vital in understanding the scale of the threat posed in a fast-moving post-incident investigation.

Through further analysis of communications data, the investigation went on to identify people who had had extensive contact with telephones used in the attack, and so enabled the security and intelligence agencies and police to ensure no further attacks were planned.

The operation led to arrests and a successful prosecution.

Northern Ireland Terrorism
Within the last three years, a group of terrorists were planning an attack in Northern Ireland. It was suspected that they had already obtained explosives for the attack and were ramping up their activity. Increased activity is often indicative of an attack being close, but the exact date was not known and the group's attention to security meant it was proving extremely difficult to discover more.

Bulk communications data provided the breakthrough. Through an analysis of the data, the security and intelligence agencies found previously unknown members of the network and were able to increase their coverage of this expanded group and were consequently aware of a sudden, further increase in activity. This led to police action and the recovery of an improvised explosive device.

It was clear that the device was ready for use and the increased activity of the group was most likely preparation for a near-time attack. A delay in the investigation would therefore likely have cost lives. Through analysis of bulk communications data the security and intelligence agencies and the police were able to arrest a key figure in the plot, who was subsequently charged and convicted for his involvement in terrorist activity.

BULK EQUIPMENT INTERFERENCE (EI)

The Investigatory Powers Bill sets out two types of equipment interference (EI) warrant – targeted and bulk. These two warrants do not authorise different powers or techniques. Rather, they both authorise the same power – equipment interference – but with different safeguards, tailored for different operational requirements and limited to different agencies.

Strong safeguards apply to any activity authorised within a targeted EI warrant and the warrant must be issued by a relevant authority after consideration of the necessity and proportionality of the interference. Where a target's devices are known, law enforcement agencies and the security and intelligence agencies may use carefully targeted EI techniques against those specific pieces of equipment. This approach constitutes the vast majority of EI operations and falls within the targeted regime.

By contrast, bulk EI techniques may need to be deployed where the security and intelligence agencies lack sufficient information to precisely target the devices of overseas suspects at the outset. Under a bulk EI warrant, the security and intelligence agencies may target a range of devices, obtaining limited data at this stage, in order to identify which of those devices are likely to be of intelligence interest. Due to the need to intrude, albeit minimally, on those who are not of intelligence interest, additional safeguards apply before data acquired through bulk EI may be read, looked at or listened to. Bulk EI warrants are only available to the security and intelligence agencies (SIA) and national security must be one of the purposes for which a warrant is sought.

Current position

The SIA have the power to undertake EI operations through the Intelligence Services Act 1994 (ISA). ISA authorisations may be for any of the Agency's statutory purposes and are issued by the Secretary of State. Section 7 of ISA permits the giving of class authorisations which do not require the authorisation to name or describe a particular piece of equipment, or an individual user of the equipment. For example, this might authorise interfering with all the smart phones across a large area to support military operations.

The bulk EI provisions in the Investigatory Powers Bill make clear that equipment interference overseas may be used in this way and enhances the statutory safeguards that apply to the use of that power.

Safeguards in the Bill

As is the case with a bulk interception warrant, a bulk EI warrant will be foreign-focused and its main purpose must be limited to obtaining data relating to "overseas-related" communications. These are defined as those communications sent or received by individuals outside the UK.

Bulk EI warrants, as well as targeted EI warrants, will continue to be issued by the Secretary of State but will now also need to be approved by a Judicial Commissioner. This will provide a new "double-lock" authorisation procedure.

The Bill will place strict safeguards on the authorisation of bulk warrants. Warrants may only be issued by a Secretary of State where he or she is personally satisfied that the activity is both necessary and proportionate. Warrants for bulk EI will last up to 6 months. The Secretary of State can renew the warrant if it continues to be necessary and proportionate and the Judicial Commissioner approves.

As is the case in respect of bulk interception, a bulk EI warrant will need to set out specified "Operational Purposes". No material or data obtained via a bulk EI warrant may be examined unless doing so is necessary for one or more of the operational purposes. Those specific purposes must be approved as being necessary by a Secretary of State and a Judicial Commissioner.

A bulk EI warrant may, incidentally, obtain communications relating to an individual in the UK. The content of communications of persons known to be in the UK may only be selected for examination under the Bill when a targeted examination warrant at Part 5 of the Bill has been obtained. The process for the authorisation of a targeted examination warrant will be the same as that for a targeted EI warrant. It will need to be issued by the Secretary of State and approved by a Judicial Commissioner before coming into force. Only the security and intelligence agencies will be able to apply for a bulk EI warrant and only in relation to three statutory purposes: in the interests of national security, for the prevention or detection of serious crime and in the interests of the economic well-being of the UK, where there is also a direct link to national security. National security must always be one of the statutory purposes for which a bulk EI warrant is authorised.

A new statutory Code of Practice will set out the handling, retention, destruction and audit arrangements for the data obtained by bulk equipment interference.

These enhanced safeguards account for the reality that in future it will not always be possible to describe target devices with the necessary high degree of specificity required for the targeted equipment regime. In such instances, the only way in which these devices can be found and identified is through what is known as 'target discovery' – using EI to acquire data from a less strictly defined set of devices, and then filtering the results of this initial EI activity. As with bulk interception, we expect that only a very small portion of the data gathered through bulk EI will be selected for examination.

The Value of Bulk Equipment Interference

The wide-spread use of communication tools and the ability of terrorists, criminal and others to exploit new internet-based technologies has made it increasingly difficult for the intelligence services to disrupt those who pose a threat. Daesh is the starkest example of how a disparate organisation has used the internet to create a near-global threat.

Historically, the SIA have largely been able to find and follow their targets through the use of interception. This capability remains critical, but technological advances is resulting in an increasing number of circumstances where interception is simply not possible or effective.

The Investigatory Powers Bill responds to this threat by providing a more transparent statutory basis for the use of bulk equipment interference.

Bulk EI facilitates target discovery by helping to join up the dots between fragments of information that may be of intelligence interest, identifying previously unknown individuals or plots that would otherwise not have been detected. Bulk EI may in some cases be the only way to acquire intelligence coverage of a terrorist suspect or serious criminal in a foreign country.

In many cases a bulk EI warrant will result in the acquisition of sufficient information to identify with a high degree of specificity subjects of intelligence interest. Once this is complete the Bill requires the issuing authority to consider if the warrant is still

proportionate. The relevant Secretary of State may then instruct that the bulk EI warrant should be cancelled.

A targeted EI operation may begin when an interception operation provides some identifying information relating to subjects of intelligence interest. For instance the SIA may learn of a specific type of device or software that is being used by a terrorist group, and the particular region within which they are operating. In this case the SIA may apply for a targeted EI warrant as they can sufficiently describe the target set and minimise the amount of data and private information acquired from unrelated devices.

However, identifying targets is becoming increasingly difficult as terrorist groups continue to use technology in sophisticated ways. For example, in another case the SIA may know of a terrorist group working in a given overseas region through reports from partners in the area but, as is increasingly the case, there may be no information available to identify precisely how members of the group are communicating with one another. In this case the SIA may apply for a bulk EI warrant focused on the geographical area. A bulk warrant would permit interference with a wide range of devices in that area in order to obtain a limited amount of data that may in itself be relatively less intrusive but which can help to identify which devices are likely to be in the possession of terrorists. This activity could not be authorised under a targeted warrant as it would not be possible to describe the devices in sufficient detail.

In this example the Secretary of State will consider the necessity of the equipment interference, and whether it is proportionate to what is sought to be achieved by the conduct. Crucially, the Secretary of State will be able to take the enhanced safeguards of the bulk EI regime in to account. Before authorising the warrant, he or she would need to be satisfied that the safeguards provided under the bulk regime mitigate the impact on persons who may not be of intelligence interest and that any collateral intrusion is proportionate to the benefits of the operation.

An authorised bulk warrant would allow the SIA to acquire information they may use to disrupt the terrorist group, whilst the enhanced safeguards minimise the impact on other individuals in the area.

BULK PERSONAL DATASETS (BPDs)

The use of bulk personal datasets by the security and intelligence agencies is a critical part of their response to the increasingly complicated and challenging task of defending the UK's interests and protecting its citizens in a digital age. The Intelligence and Security Committee said in its Privacy and Security report that bulk personal datasets are an 'increasingly important investigative tool for the Agencies'.

A bulk personal dataset is a dataset containing information about a range of people, most of whom are not of interest to the security and intelligence agencies. A list of people who have a passport is a good example of a bulk personal dataset – it includes personal information about a large number of individuals, the majority of which will relate to people who are not of security or intelligence interest. Other examples are the electoral roll, firearm licence

records, or the telephone directory. A good example of the type of dataset that might feature under a class BPD warrant (on which see below) is travel data.

Analysis of bulk personal datasets is an essential way for the security and intelligence agencies to focus their efforts on individuals who threaten our national security, by helping to identify between such individuals and eliminating the innocent without using more intrusive investigative techniques; establish links between subjects of interest or better understand a subject of interest's behaviour and connections; and verify information obtained through other sources (for example agents). It also helps the agencies to use their resources more efficiently and target potential agents.

Current Practice

The use of bulk personal datasets is not new, and the IP Bill does not provide new powers for obtaining bulk personal datasets. Section 2(2)(a) of the Security Service Act 1989 and sections 2(2)(a) and 4(2)(a) of the Intelligence Services Act 1994 – sometimes referred to as the 'information gateway provisions' – enable the intelligence and security agencies to obtain information only for the proper discharge of their statutory functions, and are the primary statutory route by which they obtain bulk personal datasets. This will not change in this Bill: as a BPD can be lawfully obtained by various statutory routes (e.g. interception and property interference as well as through the information gateway provisions), we do not consider there is a need for the IP Bill to provide for a specific power to obtain bulk personal datasets.

Safeguards in the Bill

However, the Bill provides robust and transparent safeguards around bulk personal datasets. This includes a requirement for warrants, lasting for six months, to authorise the obtaining of bulk personal datasets under (for example) the information gateway provisions. Warrants are also required to authorise the retention and selection for examination of such datasets. These safeguards are comparable to those provided for in relation to other powers under the Bill. There will be two types of warrant – class BPD warrants and specific BPD warrants. Class BPD warrants will authorise the obtaining and use of a class of bulk personal datasets, such as travel data. Specific BPD warrants will authorise obtaining and use of a specific bulk personal dataset – this could be because the dataset is of a novel or unusual type of information so does not fall within an existing class BPD warrant or because a dataset raises particular concerns that should be considered separately.

The Bill specifies that the Secretary of State must consider that the warrant is necessary and proportionate and adequate measures are in place to store the datasets securely.

The Bill also introduces a "double-lock" so that the issue of security and intelligence agencies' warrants will in future be subject to approval by both a Secretary of State and a Judicial Commissioner includes. Before a class warrant is issued, it must also be approved by a Judicial Commissioner. A specific warrant must also be approved by a Judicial Commissioner before it is issued other than in urgent cases; in urgent cases the specific

warrant must be approved by a Judicial Commissioner within five working days of being issued.

The safeguards that apply to the security and intelligence agencies' access, retention, storage, destruction, disclosure and auditing of bulk personal datasets will be covered by a statutory code of practice. All misuse of bulk personal datasets will continue to be considered to be a significant issue with the consequences of misuse still including disciplinary action and potentially criminal prosecution.

The Investigatory Powers Commissioner will also keep under review the acquisition, retention, use or disclosure of bulk personal datasets by the intelligence agencies. That is currently done by the Intelligence Services Commissioner, who confirmed in his 2014 report that the 'the case for holding BPD has been established in each service' and 'agencies all have strict procedures in place in relation to handling, retention and deletion. Misuse of data is fortunately rare. My experience is that officers work with a high degree of integrity and an awareness that the systems they have access to contain highly sensitive information which must be protected.'

The value of Bulk Personal Datasets

The following examples illustrate how the use of bulk personal datasets works in practice.

- Protection of major events. When significant events take place – such as the NATO Summit in Wales in 2014 or the London Olympics in 2012 – the intelligence services work to ensure they pass off safely. This includes tracing the details of individuals with access to venues so as to mitigate the risk that subjects of national security interest might gain access to these events. The majority of individuals in such datasets will not be of direct intelligence interest and this data is therefore categorised as bulk personal datasets.

- Preventing terrorist access to firearms. The risks of terrorist access to firearms have been highlighted by tragic events in Mumbai, Copenhagen and most recently Paris. To help manage the risk of UK based subjects of interest accessing firearms, the intelligence agencies match data about individuals assessed to have access to firearms with records of known terrorists. To achieve this, the intelligence agencies acquired multiple datasets that contained the details of individuals who may have access to firearms, even though the majority will not be involved in terrorism and therefore will not be of security concern. This allows the matching to be undertaken at scale and pace, and more comprehensively than individual requests could ever achieve. This in turn enables the intelligence agencies to manage the associated risks to the public.

- Identifying foreign fighters. Timely access to travel data has provided advance notice of the unexpected return to the UK of subjects of interest. This helps the intelligence agencies to prepare a tailored response prior to their arrival to better mitigate the threat they pose to national security. Information derived from travel data has also been critical to the ability of the intelligence agencies and their international partners

to construct an intelligence picture of individuals travelling to join Daesh in Syria and Iraq.

19 January 2016

Mr Ray McClure—written evidence (IPB0016)

I wish to make the following personal submission for consideration by the Joint Committee on the Draft Investigatory Powers Bill.

My rationale for making this submission is based on the personal experience of suffering the loss of a family member as a result of a terrorist incident (Lee James Rigby my nephew) and from forty years experience as an IT professional in financial services. Since the murder of my nephew I have had many conversations with people on privacy and surveillance issues which has shaped my views..

Today's Investigatory Powers needs to be fit for purpose for the internet age. Evil happens on the internet in many forms, Terrorists planning and executing murderous attacks, pedofiles capturing and sharing obscene images of children, drug dealers, people smugglers etc.. They all use modern communications techniques to communicate, plan and coordinate their evil. Communications such as E-mails, and electronic messages including WhatsApp, iMessager, etc.. can be created, transmitted, read and deleted in seconds. Unless these messages and their associated metadata is collected and stored and made available for law enforcement then the evidence which is required to prevent, investigate, and bring about successful prosecutions, will be lost.

1. Has the case been made, both for the new powers and for the restated and clarified existing powers?

A. The need for this legislation has been thoroughly covered in the report by David Anderson QC 'A Question Trust - Investigatory Powers Review'.

B. The report into the murder of my nephew titled "Report on the intelligence relating to the murder of Fusilier Lee Rigby" made it clear that it is beyond doubt that the attack was planned and aided by internet activity and that Internet Service Providers failed to review suspicious content and to notify the relevant authorities even when an automatic trigger indicating terrorism was activated. The sad conclusion is that we can not rely on these companies to notify and work with the appropriate law enforcement authorities. Indeed many of these companies view the security forces as the enemy and not the terrorists.

C. In the report section 401 "WHAT WAS MISSED: CONTACT WITH FOXTROT". it highlights that "some overseas CSPs do not comply with UK RIPA warrants,442 as they do not consider themselves bound by UK legislation. Therefore, MI5 cannot use its usual process in such circumstances.".

D. In section 457. the report highlights "The number of different forms of communication now available presents the Agencies with significant challenges in terms of their ability to detect and prevent terrorist threats to the UK. However, the real problem arises from the fact that most of these services and applications are hosted overseas." "CSPs based in the US have,

for the most part, refused to recognise UK legislation requiring them to provide the content of communications on their networks: they do not consider themselves to be bound by the legal obligations set out in RIPA, as UK CSPs do, and may find themselves subject to legal or civil action if they share information with the UK authorities." It is a sad to reflect that no action has been taken against any company which ignored a UK issued warrant for information, had an individual ignored a warrant that person would have faced prosecution, the same should apply to internet companies.

E. "The considerable difficulty that the Agencies face in accessing the content of online communications, both in the UK and overseas, from providers which are based in the US – such as Apple, Facebook, Google, Microsoft, Twitter and Yahoo – is therefore of great concern." To address these concerns the information must be captured and stored in the United Kingdom.

F. while I am pleased to note that THE DRAFT INVESTIGATORY POWERS BILL addresses the issue of accessing content it does little to address the issue of legally issued UK warrants being ignored by US companies.

G. However, I fear that collecting the data will not be sufficient because today all major US internet companies including Apple and Facebook, are fully encrypting their message services. Apple even boast that their encryption can not be read by the security forces. On the surface this sounds good for privacy the reality is that full encryption means full protection to any user including known terrorist and those that seek to do evil. Messaging someone in Syria does not make you a terrorist the content of the message is required. Without being able to access an unencrypted message the security forces will not be able to tell if the message is a harmless exchange of say a cooking recipe, or a set of terrorist instructions. I fear that in the name of privacy the encrypted services on the internet may lead the internet to become a safe haven for evil.

H. While acknowledging that the public have a fear of state 'spying' on their personal activities, we must also acknowledge that public accept that surveillance is a normal part of daily life, the majority of shops and every high street use CCTV, and this is accepted by the public. They are accepted because the public knows they are there for two purposes, as a deterrent to prevent crime, and as a means of gathering evidence to successfully prosecute criminals. The presence of surveillance reduces crime and improves public safety.

I. The internet is simply the largest high street and meeting place and just like the physical high street it needs to be a safe place to meet and transact business appropriately monitored and policed. Monitoring activity to prevent crime, to ensure public safety and, to gather evidence when a crime is committed, is as necessary on the internet as it is on the high street.

2. **Are the powers sought legal?**
   Are the powers compatible with the Human Rights Act and the ECHR?

   A. To me the legal context for this legislation must be based on the European Convention of Human Rights in this context the following sections apply.

   B. Article 2 - life
   Article 2 protects the right of every person to his or her life. The right to life extends only to human beings, not to non-human animals,or to "legal persons" such as corporations.

   Article 2 - The right for life - The right to preserve life, - Take life to Preserve life.

   The Court has ruled that states have three main duties under Article 2:
   - a duty to refrain from unlawful killing,
   - a duty to investigate suspicious deaths and,in certain circumstances,
   - **a positive duty to prevent foreseeable loss of life.**

      1. With article 2 the convention recognises the right to life and gives it priority over the proceeding rights including privacy. Organisations which place privacy first are wrong. A life lost can not be replaced. The human rights group Liberty who state that the loss of a few lives is a price worth paying to protect privacy show how little they value life, please do not make the same mistake.

      2. Article 2 also gives the government a duty to prevent foreseeable loss of life. The first objective of law enforcement is to prevent crime, to prevent terrorism requires intelligence, which must be gathered, analysed and used to take proactive steps to prevent these evil acts. Without the appropriate intelligence you reduce the actions of law enforcement to reaction after the event.

   C. Article 5 - liberty and security

      1. Article 5 provides that everyone has the right to liberty and security of person. Liberty and security of the person are taken as a "compound" concept - security of the person has not been subject to separate interpretation by the Court.

   D. Article 8 - privacy

      1. Article 8 provides a right to respect for one's "private and family life, his home and his correspondence", subject to certain restrictions that are "in accordance with law" and "necessary in a democratic society". This article provides a right to be free of unlawful searches.

2. Article 8 sometimes comprises positive obligations whereas classical human rights are formulated as prohibiting a State from interfering with rights, and thus not to do something, the effective enjoyment of such rights may also include an obligation for the State to become active, and to do something.

3. Article 8 makes it clear that the right to privacy has restrictions, in accordance with the law. It does allow the state to become active to do something, which does not prohibit the gathering information but access to the information gathered must be by lawful means following a warrant issued by the judiciary.

4. In the context of this draft bill I have concerns about the Home Secretary having the right to issue a warrant even with the safeguards proposed. The Home Secretary is a politician not a judge.

3. Are the powers sought workable and carefully defined?

A. I have read several times that there are concerns about the practicality and cost of the draft bill. There will be costs to implement these proposals and public companies will always challenge the costs especially where there is no commercial benefit for them. I worked in IT for 40 years over that time the amount of transactional data required to kept, and the processing demands required, rose exponentially.

B. Today, banks are legally required to keep data for years, to flag to authorities suspicious transactions to stop money laundering, customers must be validated before they open accounts and use banking services. Financial transactions are transmitted encrypted, but when necessary banks provide an unencrypted copy of financial transactions to law enforcement. We should be applying the same level of processing demands on the internet companies, there are no technical reasons not to.

C. Most of the data required is already gathered and used by internet service companies. It is used in various way from network management and capacity planning to revenue generation through targeted marketing. The volumes of data being suggested does not approach the volumes of the largest commercial databases, so volume wise there should be no problems.

D. Apple Inc. boast that their encryption can not be read by the security forces and say they are unable to give unencrypted copies of communications to law enforcement, this would not be accepted in the financial world and should not be accepted from internet companies.

E. All companies should be able to produce unencrypted message content in response to a legally issued warrant. Penalties for failing to do so should be severe.

4. **Overall is the Bill future-proofed as it stands?**

   When it comes to technology it is impossible to be future proof, new technologies are being invented every day, as it stands it is fit for purpose.

5. **Are concerns around accessing journalists', legally privileged and MPs' communications sufficiently addressed?**

   As a member of the public I fail to see why special consideration is needed for MP's and Journalists. There should be one rule for all. MP's and Journalists can, and have, committed crimes and should be subject to the same degree of surveillance as everyone else. In an open society granting special privileges to select groups only breeds suspicion.

14 December 2015

McEvedys Solicitors & Attorneys Ltd—written evidence (IPB0138)

1. This Bill: Overview and Process

1.1. Replacement of Part 1 of the Regulation of Investigatory Powers Act 2000 (RIPA), as well as the Data Retention and Investigatory Powers Act 2014 (DRIPA) is welcomed, that legislation was notoriously complex and due for review in the light of changing technology, and changing public uses. However, there should have been a fuller inquiry and frank disclosure of practices and failings –and that should have informed this process. Law Commission and other reports would have been appropriate. All due transparency and public scrutiny are called for in executing reform. The Anderson Report suffers from the limits to his brief (and duties) plus it is only one voice. This process was to be an entire overhaul but falls short and fails to start with basic principles.

1.2. There is no substantial reduction of mass surveillance powers or even their curtailment. Rather, the ability to obtain wholesale records is codified and extended to any dataset or bulk database. The proposals for it to occur in bulk and against networks plus continuous geolocation tracking, or automated profiling through the "filtering arrangements" *ring all alarms and raise every red flag in a democratic society.* Let us be clear –this is the approach of totalitarian regimes. There is no indication that the impact on millions of innocent people has been properly considered –less protected –in the Bill. Further, no evidence based case is presented for new powers[957] nor indeed any statistical research -despite the depth of the interference with the fundamental rights of the entire population.

1.3. This Bill has arisen from and against an international background of terrible abuses of public trust by security services and the serious infringement of basic human rights. These came to light at enormous personal cost to individuals who blew the whistle. Despite this, the Bill takes square aim at others who may try to come forward in future—when it should do the opposite as the public has a right to know about the systems for surveillance and its operation, and public interest disclosure is an important check against abuses particularly in light of the operational context of secrecy.[958]

1.4. The bill is peppered with references to 'proportionality,' but this is in fact a discretion (as indeed is the balancing act required when convention rights conflict) and no guidance nor proper or appropriate safeguards from arbitrary powers are

[957] It should for example be possible to compare conviction rates historically before and after mass data retention was introduced. How have other countries with and without it faired? What about historical versus current data and their relative utility?

[958] See the Tshwane Principles, No. 5 and 10 C& E.

proposed. The choices are not binary but the interests of unfettered access and expediency seem to have trumped protecting fundamental rights. This is dangerous to us and our democracy.

1.5. The short time periods together with oppressively long draft legislation –are entirely unnecessary and undesirable in light of the importance of the issues and the effect is to stifle and truncate the public debate. This is a missed opportunity to set leading standards and demonstrate rule of law. We are a gold standard legal system–and should show the way.

2. General Powers

2.1. The national security notices provision (§188) is broad and unlimited and fails to meet the test to be legally foreseeable,[959] in the letter and in spirit. Parliament must more precisely and carefully circumscribe arbitrary powers granted to the executive. Similarly, as to the technical capability notice (§189). This exceeds even the overbroad §12 RIPA 2000, which allowed the Secretary of State to order a telecommunications operator to do anything required to maintain an interception capability. It is now generalised by removal of any limitation to an interception capability. What is left is a requirement "to provide facilities or services of a specified description" where "specified" means specified by the Secretary of State in the notice. Parliament should more tightly specify the powers it grants to the executive.

3. Bulk Gathering/Surveillance

3.1. An individual has an Art.8 right to privacy, which includes a right to be protected by law from surveillance. Legislation permitting the public authorities to have access on

[959] See *Kennedy* (above) at ¶ 152 and 153 "*..especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident (see, inter alia, Malone, cited above, p. 32, § 67; Huvig, cited above, pp. 54-55, § 29; and Rotaru). It is therefore essential to have clear, detailed rules on interception … domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures (see Malone, ibid.; Kopp, cited above, p. 541, § 64; Huvig, cited above, pp. 54-55, § 29; and Valenzuela Contreras, ibid.).. contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (see, among other authorities, Malone, cited above, pp. 32-33, § 68; Leander, cited above, p. 23, § 51; and Huvig, cited above, pp. 54-55, § 29). 95. In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed (see, inter alia, Huvig, cited above, p. 56, § 34; Amann, cited above, § 76; Valenzuela Contreras, cited above, pp. 1924 -25, § 46; and Prado Bugallo v. Spain, no. 58496/00, § 30, 18 February 2003)."153. As to the question whether an interference was "necessary in a democratic society" in pursuit of a legitimate aim, the Court recalls that powers to instruct secret surveillance of citizens are only tolerated under Article 8 to the extent that they are strictly necessary for safeguarding democratic institutions. In practice, this means that there must be adequate and effective guarantees against abuse. The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by the national law (see Klass and Others, cited above, §§ 49 to 50; and Weber and Saravia, cited above, § 106)..*"

a generalized basis to electronic communications compromises the essence of this fundamental right, see Case C-362/14, *Maximillian Schrems v Data Protection Commissioner.* Art 10 is also engaged when the public's right to receive and impart information is impacted and the proposals are chilling *per se* –given the bulk and indiscriminate mass surveillance and lack of limits on time or use—this literally impacts all speech and expression. See *Liberty and Others v. the United Kingdom*, no. 58243/00, ¶56 to 57, 1 July 2008 (the mere existence of a regime for surveillance measures entailed a threat of surveillance for all those to whom the legislation could be applied). The starting point is a basic right to judicial process (Arts. 6[960] & 13). This should be approval by a neutral and detached judge or magistrate before *individualized* collection or *individualized* use in a current investigation.[961] Let us be clear given the Bill is to reform—the starting point from which departures must be measured is prior *individualized* judicial authorization by warrant.

3.2. The "bulk" provisions give unfettered mass surveillance powers to the intelligence services. There was already very wide discretion under earlier and more detailed processes stipulated in RIPA and we cannot conceive how this new approach is consistent with recent law ---see *Kennedy v. UK,* 26839/05, and *Zakharov v. Russia* 2015 (47143/06) [GC].

3.3. The distinction between content and metadata (§193) and the reduced protection for the latter is flawed--metadata may allow "*very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained"* and the retention of metadata relating to a person's private life and communications is, in itself, an interference with the right to privacy, see cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others* and *Copland v the United Kingdom,* No 62617/00 ¶¶ 43-44; cf. *Rotaru v Romania*, No 28341/95, Judgment (GC) ¶ 46 (same). We note and abhor the lack of specificity in the Bill about what constitutes metadata and therefore receives no protection. This should be precisely defined, in particular, in relation to live and historical location data.

3.4. Equipment interference, as detailed in Part 5 and, as a "bulk" power, in Part 6, is an extremely intrusive form of mass surveillance, seriously interfering with the right to privacy. It can yield information sufficient to build a total profile of a person, from his daily movements to his most intimate thoughts. The UN Special Rapporteur on freedom of expression noted *"individuals regularly hold opinions digitally, saving their views and their search and browse histories, for instance, on hard drives, in the*

[960] Art 6 starts: *"In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly…"*

[961] See *Kennedy v. UK,* 26839/05 at ¶167. "*The Court recalls that it has previously indicated that in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge (see Klass and Others, cited above, § 56)."*

cloud, and in e-mail archives, which private and public authorities often retain for lengthy if not indefinite periods." This implicates Arts. 9 and 10. The intrusion involved and the risk to security of communications raises such serious human rights concerns that a high standard of scrutiny and proper judicial authorization must be required. Instead, Part 5, the supposedly "targeted" hacking provision, permits attacks on broad categories of equipment that could include that belonging to communications service providers. Part 6 (3) of the Bill compounds this problem by allowing hacking to be carried out "in bulk" when it is directed overseas.

3.5. Abuses in the past and new research reveal ordinary activists, NGOs and human rights' defenders have been targeted by equipment interference attacks. Often their work is very clearly in the public interest and yet the Bill is silent as to meaningful measures likely to provide any safeguards or protections for these groups—despite the public interest in the debates they engender and their crucial role in democratic societies.

4. <u>DPI/Blocking</u>

4.1. Under RIPA, actions by telecommunications operations that would otherwise constitute an unlawful interception were authorized if are a necessary part of the provision of the service (RIPA §3(3)) and this is preserved in the Bill (§33(2)(a)). However, the Bill also adds that a telecommunications operator is authorized to intercept without a warrant: "*for the purpose of any enactment, or for the purpose of "preventing or restricting the viewing or publication of the content of communications transmitted"* (§33(2)(a)). Essentially, this removes the legal impediment to ISPs from conducting Deep Packet Inspection (DPI) so as to inspect customer traffic and decide whether to block it—the absence of this previously prevented ISPs from accommodating informal government or police requests to block access to certain content as ISPs refused to act without legislative protection/authorization due to the earlier legal prohibitions on unlawful interception. While the new provision enables the blocking of content which is illegal (mainly, child abuse imagery and certain terrorist content) and may also extend to content that is the subject of civil claims (say intellectual property infringements or defamation) it can encompass the blocking of perfectly lawful content without any court order or judicial scrutiny and impact fundamental Art 10 rights. The potential for misuse and its significance are obvious. This is a slippery pole as many others will clamor to use such powers once in place—as the developing law on internet intermediaries demonstrates. The law enshrines valuable protections against prior restraints on speech --*even from interference by the courts*. The risks posed by this new power must be considered more carefully and be contained and proscribed as appropriate in light of the seriousness of these issues.

5. <u>Data Retention</u>

5.1. The provisions related to retention (Part 3 and Part 4 of the Bill), particularly in relation to the capacity to obtain “Internet Connection Records” and the powers to require blanket and unlimited retention of communication data appear to be in violation of current law. Indefinite retention is offensive to law per see, see *S v Marper* ([GC] 30562/04 ECHR) (retention of DNA samples of individuals not charged or convicted of a criminal offence, a "disproportionate interference" with private lives (¶135) due in part to lack of any assessment of suspicion). See also *Google Spain* C131/12 and the right to be forgotten as an aspect of Art. 8 rights.

5.2. The 2006 Data Retention Directive (Directive 2006/24/EC) which required communications service providers (CSPs) to retain customer data for up to two years for the purpose of preventing and detecting serious crime, breached the rights to privacy and data protection and was quashed in C-293/12, *Digital Rights Ireland v Minister for Communications and others.* The Grand Chamber observed that the scope of the data retention "*entails an interference with the fundamental rights of practically the entire European population*" (¶56). The Court went on to note the Directive was flawed for not requiring any relationship between the data whose retention was provided for and a threat to public security (¶59) and found it amounted to a "wide-ranging and particularly serious interference" with the rights to privacy and data protection "without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary". Data preservation must be based on suspicion.

5.3. The Bill fails to anticipate the forthcoming revised regime in the EU and is therefore premature and while there may be a perceived urgency due to the sunset clause on DRIPA (2014), we are concerned that if we rush into substantial new legislation in the UK it may have barely reached the statute book before we are forced to consider supervening EU instruments.[962]

5.4. The mandatory data retention regime under the Bill will go much further than the old Directive—in so far as it will not only be limited to the detection or prevention of serious crimes, but for any of the grounds under which communication data can be requested (§46.7) and, it seems, for any other purposes whatsoever (§5(2) and (3)). While the Judicial Commissioner is to check proportionality in appeals, no prior or subsequent judicial authorization is required for retention orders. There is also no explanation of how transition issues will be handled in relation to legacy datasets.

5.5. We strongly oppose the acquisition of datasets and particularly as to communications data. The Bill will facilitate access to dozens of public bodies. The

[962] See also *David, Watson et al v Secretary of State for the Home Department* [2015] EWHC 2092 (Admin) *(*DRIPA ceases to apply from March 2016) now referred to the CJEU as to whether it intended in *Digital Rights Ireland* (above) to set controlling standards for Member States.

potential for abuse is just too great and there is no realistic possibility of meaningful supervision. We refer to the local authority misuse of RIPA for checking address information for school places purposes. All databases should be out of government hands with clear prior request and judicial authorization procedures for particular data and a publication scheme for information on the nature and number of requests. The Bill contains provisions that would appear to enable the intelligence services to routinely obtain databases and carry out initial examinations in order to determine their usefulness without any warrant and then retain that data and use it as it sees fit without a valid warrant (§150). The guidelines also contain troubling indications that low level officials may obtain data without consulting senior staff compounding the issues in practical terms.

5.6. The Bill allows the Secretary of State to authorize data retention notices without any judicial authorization. Only if there is a review of the retention notice, on referral by a telecommunication operator, does the Secretary of State need to consult the Investigatory Power Commissioner (IPC), although he is not obliged to accept his recommendation(s) (§73). This ignores the lessons from the Digital Rights Ireland case, where the Grand Chamber noted - finding a violation with the rights to privacy and data protection enshrined in Articles 7 and 8 of the Charter - that *"above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions."*

5.7. Further, this is an area where precise hard law is crucial and should be employed to protect the data and its processing -and codes of practice should be avoided. With respect to Part 7 of the Bill as to Bulk Personal Datasets (BPD), ¶74 of the general preamble proposes: “A statutory Code of Practice will set out additional safeguards which apply to how the agencies access, store, destroy and disclose information contained in the BPDs”. The BPD Code is proffered as a key safeguard in addition to the so called “double lock” however we have no draft BPD Code of Practice. So called ‘safeguards’ (§§117, 131, and 146) are therefore absent or inadequate. A lack of minimum statutory safeguards to protect against arbitrary interference and abuse, violates the requirement of legality under international human rights law. We refer to the UN Human Rights Committee recommendations to the UK in July 2015 to: *“ensure that any interference with the right to privacy, family, home or correspondence is authorized by laws that: [...] (iii) are sufficiently precise and specify in detail the precise circumstances in which any such interference may be permitted, the procedures for authorization, the categories of persons who may be placed under*

surveillance, the limit on the duration of surveillance; procedures for the use and storage of data collected."

5.8. There are particular concerns about sensitive personal data, such as medical records, and the provisions in the guidelines are soft and not hard law and vague. The Bill must restrict access and use of data recognized as sensitive in data protection legislation. The provisions as to interception in hospitals (§38) is totally incompatible with Art 8.[963] While the data protection regime is not strictly applicable,[964] it should inform.

6. Filtering

6.1. The "filtering arrangements" (§§14-16) were understand are best understood as a "profiling engine" which creates detailed profiles on all users of electronic communications systems and makes those profiles available for sophisticated data mining –an enormously powerful and intrusive tool for public authorities. Its mere existence significantly implicates Art. 8 privacy rights, and its extensive use would represent a dramatic shift in the balance between personal privacy and the capabilities of the State to intrude on the citizen. This is not correctly characterized a safeguard.

6.2. When used in a targeted and individualized judicially authorized way or even against persons appropriately already of interest who would otherwise come under intrusive investigation anyway, this kind of technique might be considered proportionate. However, we note that it is the purpose of this legislation to keep voluminous, intrusive and potentially intimate records on the entire population. It could be misused to score the entire population for potential to have been involved in a crime, or other permitted areas of enquiry? The nature of the data potentially to be gathered is such that scores could be constructed for example, to assist an investigation by H.M. Revenue and Customs into whether the target's lifestyle matched their reported income. This needs the most careful consideration and limitation.

7. Judicial Commissioners

[963]See *Peck v UK* 44647/98, *W v Egdell* [1990] Ch 359 (psychiatric report protected by confidence) and *Kaye v Robertson* [1991] FSR 62 (malicious falsehood where no consent to images taken in hospital).

[964]While since 1984, the national security function has been largely exempt from data protection (§28 of the DPA), this can require a certificate to be signed by the Secretary of State, such section 28 certificates appear to be timeless, see the *Privacy International* case ([2014] UKIPTrib 13_77-H; (05/12/2014) at ¶19) (GCHQ produced a certificate signed by David Blunkett thirteen years previously (in 2001) to show that key obligations in the Data Protecting Act were exempt).

7.1. These commissioners lack full independence and are somewhat captured. This reduces appropriate neutral and detached judicial oversight. Only the ordinary courts can provide the independence necessary –via ordinary serving and rotating judges sitting in the higher courts. Rulings must be public and hearings adversarial—with adequate protections when needed. The independence of judges is a key consideration –see *Zakharov v. Russia* 2015 (47143/06) [GC] (where although the system required prior judicial authorization (¶259] it was not sufficiently independent nor able to counter the breadth of the state powers). So even where there is individualized prior judicial authorization –that is not a free pass for surveillance systems. Similarly, such commissioners had several earlier incarnations. So few complaints have succeeded in the past under the earlier manifestations which demonstrates they are not fit for purpose –particularly in light of the systemic abuses and failures driving this new round of reforms. Judicial authorization in a civilized and advanced society should require:

(i) a showing of probable cause a specific serious crime has/is been committed;[965]
(ii) be in relation to named persons;
(iii) describe particular communications;
(iv) be limited to a short period of time;
(v) with provisions for its termination
(vi) provide for a return to court to show what has been obtained/intercepted.

7.2. As applied in a national security context see *Zakharov v. Russia* 2015 (47143/06) [GC] (minimum standards include stipulation of: "[t]*he nature of offences which may give rise to an interception order; A definition of the categories of people liable to have their telephones tapped; A limit on the duration of telephone tapping, Protections and procedures for use, storage and examination of resulting data; Safeguards relating to the communication of data to third parties; Circumstances in which data/recordings must be erased/destroyed (para 231));* there the General Court found that equipment installed by the secret services kept no logs or records of intercepted communication, which coupled with the direct access rendered any supervisory arrangements incapable of detecting unlawful interceptions and held the emergency procedure provided for in Russian law, which enables interception without judicial authorization, did not provide sufficient safeguards against abuse"). If not prior to gathering—judicial approval must be prior to *individualized* use in a current investigation. Failure to comply should mean the evidence is excluded ---in order to educate and provide effective sanction for failure and promote lawful gathering. The indiscriminate procedures for bulk warrants (Part 6 and Part 7 of the Bill) offend these basic principles and are grossly untargeted, overbroad, vague and

[965] See *Gillan & Quinton v United Kingdom,* 4158/05 ECHR at ¶85 (intrusive power with broad discretion that did not require any reasonable suspicion, here random stop and searches under s44 of the Terrorism Act 2000, gave rise to a "clear risk of arbitrariness")

the purposes arbitrary and secret --not proportionate or necessary in the interests of national security. It is difficult to see how these proposals can possibly be compliant with established law.[966]Thematic warrants e.g. in relation to: *"[a] group of persons who share a common purpose or who carry on, or may carry on, a particularly activity,"* do not require individuals to be named (or even known) --similar to general warrants outlawed 250 years ago.

7.3. As to the so-called "double lock," (§84.1) with all due respect, the executive is not a check on itself. [967] Nor can any distinction be relied upon between enforcement and the executive in times of pressure or crisis --as the Huhne and Mitchell affairs demonstrated by police avoidance of PACE and its protections in order to seize journalistic materials under RIPA. See §§19-21, 59, 90, 109, 123, 138, 155.

7.4. Worse, when authorization is required in the Bill, these 'Judicial Commissioners' are only required to apply the "same principles as would be applied by a court on an application for civil judicial review" –namely *Wednesbury* unreasonableness or irrationality (§§19.2, 109.2, 123.2, 138.2, 155.2) and not the standard appropriate in a criminal context –such as detailed in *Zakharov* (above). This will limit the review to procedural aspects (as it has in the past). This is exacerbated by the inherent dangers in "bulk" processes, namely that authorization requests will be formulated so broadly as to make assessments challenging. Further, necessity and proportionality assessments need only take into account "whether the information which it is considered necessary to obtain under the warrant could reasonably be obtained by other means" (see §§14.6, 107.5, 122.4 and 137.4) and not the appropriate standard of whether other less invasive techniques have been exhausted or would be futile, such that the techniques used is the least invasive option.

7.5. Local authorities are required to apply for authorization but it is not appropriate for this to be to a justice of peace, a sheriff or a district judge (§59), it must be to a High Court Judge given the complexity and the heightened need for scrutiny and the nature of the applicant. The continued commitment to oversight by Single Points of Contact, one of the more successful innovations under RIPA, is welcomed by many (§60) but should not work against the principles of independent scrutiny.

---

[966] See *Kennedy v. UK,* 26839/05 at ¶160 "*Finally, the Court notes that in internal communications cases, the warrant itself must clearly specify, either by name or by description, one person as the interception subject or a single set of premises as the premises in respect of which the warrant is ordered (see paragraphs 40 to 41 above). Names, addresses, telephone numbers and other relevant information must be specified in the schedule to the warrant. Indiscriminate capturing of vast amounts of communications is not permitted under the internal communications provisions of RIPA (cf. Liberty and Others, cited above, § 64). The Court considers that, in the circumstances, no further clarification in the legislation or the Code of the categories of persons liable to have their communications intercepted can reasonably be required."*

[967] See as to the safeguards and the arrangements put in place by the Secretary of State under section 15 RIPA, the circularity in the fact that the person responsible for issuing warrants was also responsible for the establishment of the safeguards—cited by the court in *Kennedy* (above) at ¶ 134.

7.6. The lack of notification obligations and the strict prohibitions on disclosure, deny individuals the knowledge and ability to seek redress for unlawful surveillance. A monitoring scheme will not be 'in accordance with the law' if it fails to ensure that persons who are monitored are notified of the surveillance (if only ex post facto), see *Assn. for European Integration and Human Rights & Ekimdzhiev v Bulgaria*, 62540/00, a t ¶ 90-91. While the Bill envisages the continuation of the ability for the public who believe they have been the victim of an abuse of investigatory powers to lodge a claim with the Investigatory Powers Tribunal (IPT), the individual will normally remain unaware of being subject to covert surveillance, authorized or not, and RUSI pointed to the systemic weakness of the IPT in that errors only come to light after claimants make an application to the tribunal. While there is new provision for 'error reporting' (§171), the IPT has minimal investigatory resources and relies for most of its information on that provided by the agencies. This is clearly inadequate. Experience abroad indicate extra-parliamentary oversight bodies find that the investigation of specific complaints provides a detailed insight into agencies operations and complement review activities. Individuals should be notified of a decision authorizing their surveillance with enough time and information to enable them to challenge the decision in a hearing or seek other remedies and should have access to the materials presented in support of the application for authorization. An express duty of full disclosure and good faith should be imposed on the services seeking to delay notification. Delay in notification should only be appropriate on a showing that notification would seriously jeopardize the purpose for which the surveillance is authorized, or there is an imminent risk of danger to human life; and authorization to delay notification is granted by a judicial authority. Further, communications service providers should be allowed, with limited exception, to notify individuals. Surveillance data must be made available to criminal defendants and the prohibition on this removed (§42). This is another crucial check and balance but also the point at which violations of law impact the rights of the individual and their Art.6 rights most significantly.

8. <u>The Investigatory Power Commissioner –IPC</u>

8.1. The merger of the different RIPA Commissioners into an Investigatory Powers Commissioner is welcomed as the separation was confusing to the public, and created the potential for duplication. More importantly, it reduced transparency and undermined the ability of any of them to build public confidence in the investigatory powers. This merger of the existing three commissioners is one of the better features of the Bill. Further, the IPC is defined functionally instead of in terms of specific agencies and the Bill covers all empowered to conduct covert investigations. The Intelligence and Security Committee (ISC) we understand will continue to oversee policy, administration, expenditure.

8.2. However, the main flaw in the Bill is that the IPC conducts both authorization and oversight: this combines two functions that should be kept separate. This goes entirely to the heart of the Bill. We note, the Bill is the first occasion that intelligence control and oversight issues have been addressed holistically as the commissioner/tribunal was first initiated in 1985 and has grew incrementally until RIPA gave us comprehensive legislation on the authorization of covert intelligence - to ensure compliance with the Human Rights Act 1998-- but retained the piecemeal system for oversight that had developed to that point. Public confidence in the acquisition and retention of data rests on the credibility and practicality of the legal and oversight frameworks.

8.3. The Bill imposes on the IPC, specific duties to law enforcement and security interests. See his duties to avoid acting in a way contrary to the national or prejudicial to the national security, the prevention or detection of serious crime or the economic well-being of the UK, under §169(5), and to avoid jeopardizing the success of an intelligence, security or law enforcement operation, under §169(6). Unless more specific duties are laid upon him requiring him specifically to consider and report on the proportionality of practices and capabilities under review (including, especially, new practices and new capabilities) the Commissioner's duties to law enforcement may well inhibit him from transparent reporting. In particular, he may feel inhibited reporting on and bringing to Parliament's attention any objectionable or unlawful practices. Like everyone else with duties under this Bill, he is bereft of statutory guidance or statutory principles to apply in considering the proportionality of the matters he is supposed to keep under review.

9. <u>Individuals entitled to Equal Protection</u>

9.1. MPs absolutely should not be entitled to any greater protection than members of the public (§16). This is crucial -they must share precisely the deprivation of privacy suffered by the citizen in order to incentivize them to guard our liberty, rights and freedoms and similarly, they can share the chill that the lack thereof will bring to expression.

10. <u>Sources and Privilege</u>

10.1. The Bill offers wholly inadequate protection for journalists and their sources (§61)—a serious threat to the vital press function as a watchdog of democracy. For the press to operate as a watchdog of democracy, it needs sources and there is a constant interest in protecting the same –even in a security context and even where there are threats to life. See Art. 10 and *Goodwin v UK* (1966) 22 HRR ("*Protection of journalists sources is one of the basic conditions of press freedom…without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result, the vital public watchdog role of the press*

may be undermined. Having regard to the importance....and the potentially chilling effect an order of source disclosure has on the exercise of that freedom, such a measure cannot be compatible with Art.10..") and *Saint Paul Luxembourg SA v Luxembourg*, 26419/10 (warrant for search of newspaper office breached both Arts 8 and 10). It is difficult to see how this can be reconciled in a meaningful way with the bulk acquisition and processing regimes in Part 6 of the Bill. The inadvertent collection of data on and from journalists and the temptation to access it without advance authorization in times of national or executive stress will be too great. See again the Huhne and Mitchell affairs. Further, the safeguards extend only to police and not intelligence services. This should also all be hard law not a code of practice as proposed. Journalists should not be prosecuted for receiving, processing or publishing classified information in the public interest and must also be properly protected from the offences (see further below). See Tshwane Principles Nos. 47 & 48.

10.2. We welcome that the secrecy rules relating to interception have been adjusted to allow telecommunications operators to ask for, and receive, professional legal advice in relation to their obligations (§43(5)(f)). However, we are yet to see adequate protection for legal privilege from bulk gathering, storage or use.

11. Internet Connection Records and Third Party and Entity and Location Data

11.1. The new "Internet Connection Record (ICR)" has no precise technical status and any analogy with phone records ("x accessed Facebook at 1.34pm") is completely misleading as it is not possible to collect this data without touching and processing "content". Likewise, third party data implicates content and the depth of the intrusion is extreme and cannot be justified except on a targeted basis with proper prior judicial authorization

11.2. Mr. Anderson QC, said in his report, A Question of Trust, *"[t]here should be no question of progressing proposals for the compulsory retention of third party data before a compelling operational case for it has been made out (as it has not been to date) and the legal and technical issues have been fully bottomed out*." The response is this concept in the Bill of ICRs –which appear to be records of which websites (or other Internet-based service) a user has visited, but do not includes details of what they have done using that service. To take Mr. Hutty's example; "*consider a person who is a BT Internet-access customer who uses Facebook to send a message to another person. Requiring BT to collect third party communications data would require BT to collect details of that message including, inter alia, the fact, time and recipient of the message. By contrast, collecting Internet Connection Records would only require BT to identify and record that their user had visited, at a given time, the Internet Protocol address that is used by Facebook."*

11.3. We agree and concur with others who have raised serious doubts about whether it is possible to draw a distinction between merely identifying that Page 9 of 19 was accessed without disclosing any meaning from the communication itself and refer to the excellent example given by Mr. Hutty: "a. Internet Connection Records might show that a user had repeated access over a period to the following web sites:

i. http://www.thewhiskeyexchange.com/
ii. http://www.masterofmalt.com/
iii. http://www.liqor.com/
iv. https://uk.thebar.com/
v. http://alcoholicsanonymous.com/ "

The level of additional intrusion is enormous and can only be justified on a narrow targeted basis following prior full judicial authorization based on probable cause of specific and extremely serious offences –that is, as detailed in *Zakharov* (above). A greater proportion of people's lives are lived "online" than when RIPA 2000 was enacted so here is a much richer range of communications data to be had. Further, enormous progress has been in recent years in analyzing large data sets to draw inferences about every aspects of individuals lives.

11.4. CSPs are being asked to develop their own solutions for this and to process user data to provide information the government wants to have rather than simply retaining information in the normal course of business. We know from the hacking cases, that these records are cheaper than phone records to acquire but much more intrusive –indeed the creation of ICRs would almost certainly require intrusive monitoring that should be classed as interception rather than acquisition.

11.5. Compounding these concerns is the fact that companies that now fall within the new definition of a telecommunications operator include such social networking and messaging services as Apple, Facebook, Google, Microsoft, Yahoo! and everything they know about anyone will be considered "Entity" data, other than that which is "Events" data. Accordingly, the power to require telecommunications operators to give access to communications data includes access to anything that Google, Facebook and Apple hold on anyone. The Bill does not make any attempt to segregate different types of entity data or make differential provision for access according to the level of intrusion. We consider this totally inconsistent with the rule of law and *Zakharov* (above) standards.

11.6. As to Location Data, we consider it grossly disproportionate and inappropriate for telecommunications operators to be required to keep near-continuous and potentially substantially complete geolocation records of the movements of

essentially the entire population of the UK and refer to comments already made about safeguards and standards prior to individualized use.

12. Security Risks

12.1. We do not support requiring telecommunications operators to build "backdoor access" into what ought to be strong end-to-end encryption protecting customer communications. The security such encryption provides is very much to the benefit of the UK, and introducing deliberate vulnerabilities of this, or any other nature, would be most unwise and exposes the public and businesses to serious data and financial risks. Once compromised, it may not be possible to contain the damage.

12.2. In §189(4)(c) there is a reference to one of the obligations that may be imposed on a telecommunications operator being "the removal of electronic protection applied by a relevant operator to any communications or data". a. This particular provision has been the subject of much press comment and speculation; some of it no doubt ill-informed, but some of it carrying the air of a government background briefing. b. It is suggested that this phrase in particular, and s189 in general, is intended to empower the Secretary of State to require telecommunications operators to provide "backdoor access" to their services, bypassing encryption that normally protects customer communications.

13. Sharing and Mutual Assistance Frameworks

13.1. Foreigners must have the same protections as UK citizens --to protect from the previously exposed abuse of unfettered sharing of data gathered by co-operating governments whereby the US gave their data on UK citizens to the UK and the UK gave their data on US citizens to the US –*making a total mockery of all safeguards, limits or protections.* We note the data may again be transferred overseas "*to the extent (if any) as the Secretary of State consider appropriate*" (§118.2). A transparent and rule based mutual sharing framework must be provided for with reciprocal protections and standards required –as in the civil law data protection regime. There should also be prior judicial oversight before transfers and the *Zakharov* (above) standards applied to them. Part 6(3) of the Bill for example allows hacking to be carried out "in bulk" when it is directed overseas. This is totally unacceptable and given the international journey of even domestic messages – threatens again to make a mockery of all safeguards.

13.2. Note bulk interception warrants related to communications sent or received by individuals outside the UK (§§106-121) and the (§§111.4) general purposes and inadequate safeguards to be followed for examining, sharing, retaining and deleting material or data obtained under the bulk warrants – all too broad and vague to provide sufficient guidance and prevent abuse (§§117). In particular, the disclosure

of information obtained under a bulk warrant is broadly permitted so long as the information is or is likely to become necessary in the interests of national security or other relevant grounds. Similarly, provisions regulating destruction of material or data obtained through bulk warrants would allow the retention of such data indefinitely and (§119) intercepted materials can be examined without limitation, in so far as it is necessary for the purposed specified in the bulk warrant, which is likely to be too general. This fails current legal standards, see above.

13.3. We note that the Bill purports to impose obligations in Parts 2, 3 and 4 on telecommunications operators outside the UK. We consider this to be wrong in principle and likely to cause great difficulties in practice. The assertion of extra-territorial authority will rob the United Kingdom of a principled basis for dissuading or criticizing foreign governments from following this precedent, and will indeed encourage such behavior. This will diminish British sovereignty in the long run.

14. Offences, Whistle-blowers, Tipping and Transparency

14.1. The Bill should include procedures for internal and external public interest disclosures. This is a crucial protection for whistle-blowers.

14.2. The offences in the Bill must also provide express public interest defences. Failure to do so denies protection for whistle-blowers. The press and the public need these as another check against repeats of the past abuses and misuse of public trust. Recent comparative studies of G20 countries describe the status of national intelligence and defence in the UK as a "glaring gap" in the legal framework protecting whistle-blowers. Without amendment, the new offences in the Bill will have the effect of widening rather than narrowing that gap to make CSP employees and contractors subject to Official Secrets Act-type restrictions and penalties. This is shameful. We should lead and not lag.

14.3. The Tshwane Principles were published on 12 June 2013, six days after the first report based on Edward Snowden's revelations was published, and following two years of work. They were based on a survey of national and international legal standards and informed by discussions with 500 experts from 70 countries. The Principles provide guidance on information of "high public interest", such as statistics on the extent of surveillance practices. They state that whistle-blower protections should extend to national security disclosures under certain conditions and disclosures in the public interest should be protected from retaliation. Where individuals are prosecuted for the disclosure of information over and above that required in the public interest any punishment must be proportional to harm caused by the disclosure. The Parliamentary Assembly of the Council of Europe (PACE) endorsed the Tshwane Principles in October 2013. The Committee of Ministers also adopted a recommendation on the Protection of Whistle-blowers that recognizes

that, while member states may institute "a scheme of more restrictive rights" for information related to national security, defence or international relations, *"they may not leave the whistle-blower completely without protection or a potential defence."* In a resolution of May this year, the Parliamentary Assembly went further and recommended asylum should be available for national security whistle-blowers whose disclosures have not been treated in accordance with the Tshwane Principles. David Kaye, the UN Special Rapporteur for the Promotion and Protection of the Right to Free Expression, in his report of 8 September 2015 concurred that while states should avoid prosecuting whistle-blowers, where this happens, defendants *"should be granted ... the ability to present a defence of an overriding public interest in the information and ... access to all information necessary to mount a full defence, including otherwise classified information."* In March 2014, the European Parliament adopted the conclusions of an inquiry into surveillance practices conducted by the LIBE committee. Among its many recommendations, this report recommended that the Commission consider the possibility of establishing guidelines for national security whistle-blowers across the EU and called on member states to ensure their national frameworks were in accordance with international standards, including the Tshwane Principles. See also the Tshwane Principles Nos. 40, 41 & 43& 46. Public sector whistle-blowers have particular protection under Art.10 and from criminalization.

14.4. Protections should also extend to security researchers working in the public interest to avoid ambiguity around the practices of computer security research, whereby freelance computer security experts search for, analyze and report on vulnerabilities in the systems of technology firms, sometimes in response to incentives from prominent technology companies, as an integral part of troubleshooting and perfecting network security. Researchers working in this field already face legal uncertainty. The wording in the present bill potentially criminalizes this important work.

14.5. The criminalization of tipping is also troubling, see §§43-44, 66, 77, 102, 133, 148 and 190. While RIPA 2000 already had tight provisions governing the secrecy of interception capabilities, these have been extended to cover new areas. Under the Data Retention Directive and its temporary replacement, DRIPA, the data types ISPs were required to retain were visible on the face of legislation. Under the Draft Bill, by contrast, a telecommunications operator must keep secret what they are required to retain and indeed the very existence of a retention notice. We recognize the importance of protecting operational security and agree that legal restrictions should be placed on telecommunications operators preventing them from “tipping off” the subject of current investigations. We also agree that is would be irresponsible to disclose certain details relating to investigation capabilities, in

particular weaknesses in or limitations to more general capabilities that are more widely expected. That said, we do question whether it is healthy for the democratic process to conceal the overall picture of the state of general surveillance of the population in the UK from Parliament and the courts.

14.6. The ISC actually called for greater openness. Concerning targeted warrants, the ISC recommended that, contrary to the blanket prohibition under RIPA, "*disclosure [of a specific interception warrant] should be permissible where the Secretary of State considers this could be done without damage to national security.*" We consider §66 in particular, would be better framed as a general expectation that orders for communications data will become public at some point in the future, subject to an official veto where it is operationally necessary. The three provisions relating to targeted warrants, and the criminalization of notifying the subject of a notice—indeed --notifying "anyone;" may inadvertently prevent CSPs from releasing aggregated, anonymized information about the official requests they receive. In recent years, an increasing number of communications service providers have started releasing transparency reports, which have done a great deal to improve public understanding. Indeed, in the aftermath of the NSA scandal, a number of CSPs in the US reached an agreement with the US Government, allowing data on official orders to be disclosed in a set format. Enabling CSPs to release this kind of comparative data would provide an important complement to the information currently issued by IOCCA. Nothing should prevent CSPs producing their own Transparency Reports. Where such international, anonymized and aggregated data is available, this provides an important complement to the information currently issued by UK authorities.

14.7. Section 77 imposes a duty for "a telecommunications operator, or any person employed for the purposes of the business of a telecommunications operator" not to disclose the existence or content of a data retention notice. While the duty to comply with a data retention notice is not new, the duty to keep secret the "contents" of such a notice is - under the Data Retention and Investigatory Powers Act (2014), augmented with a provision in the Counter Terrorism and Security Act (2015), the categories of data that ISPs are obliged to retain are explicitly set down in law. The Bill is considerably more opaque in this respect, not least due to the ambiguity as to what constitutes an ICR. A strong case needs to be made for imposing secrecy where information was formerly available, particularly as this impacts the Arts 8,9 and 10 rights of all who use a UK ISP. For bulk orders, "tipping off" is not a concern as such orders will affect a large number of individuals (not suspected of any wrongdoing whatsoever) so a permanent prohibition on revealing anything about these orders, which are matter of intense public concern and directly

and seriously impact fundamental rights, is unnecessary and disproportionate and likely to inhibit important public debate in the public interest.

14.8. We welcome the introduction of a new offence that can be committed by misusing a position in a public authority to gain access to communications data unlawfully (§8). With extraordinary powers comes extraordinary responsibility, and it is important that those who betray that trust can be seen to be held accountable. The principle of criminal accountability for misuse of public powers is an important one, whose introduction we would welcome in other similar situations.

22 December 2015

medConfidential—written evidence (DIP0005)

1 medConfidential is an independent non-partisan organisation campaigning for confidentiality and consent in health and social care, which seeks to ensure that every flow of data into, across and out of the NHS and care system is consensual, safe and transparent.

2 Our comments are limited to issues relating to Bulk Personal Datasets (Part 7 of the Draft Bill), however, we note that some language is replicated for Bulk Communications Datasets, and that recommendations for one part should be considered for replication in the other.

Summary

3 Much of the focus of the Bill scrutiny has been on the important topic of communications and interception. However, Bulk Personal Datasets cover everything else electronic that isn't communications: the administrative records that organisations keep to conduct their affairs. The Agencies want the ability to acquire, covertly or overtly, any dataset used here or overseas:[968]

4 "The information on individuals within Bulk Personal Datasets *"...may include, but is not limited to,* ***personal information such as an individual's religion, racial or ethnic origin, political views, medical condition, ***, sexual orientation, or any legally privileged, journalistic or otherwise confidential information****"* – para 163(ii), p58, ISC report

5 *"A bulk personal dataset (BPD) is a dataset containing information about a wide range of people..."* which *"...includes a large amount of personal information,* ***the majority of which will relate to people who are not of security or intelligence interest."*** [969] – para 1, Home Office, BPD factsheet published 4 November 2015

6 The power is effectively unlimited, the scope unlimited, and the side effects unconsidered.

7 With these great powers, comes absolutely no responsibility whatsoever to any body outside the hierarchy of command, meaning no oversight.

8 Not only should the use of bulk medical records of groups for intelligence purposes be entirely disavowed by all agencies as a collective intrusion and breach of human rights, it should be explicitly legally prohibited in this Bill. The Home Secretary said she wanted a "world-leading oversight regime",[970] but there must be things that are both disavowed and explicitly prohibited by "world-leading" democracy.

---

[968] while Part 6 of the bill allows Bulk Communications Data to be shared overseas (clause 40(7)) the Bill is silent on similar arrangements for Bulk Personal Datasets.

[969] Factsheet: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473750/ Factsheet-Bulk_Personal_Datasets.pdf

[970] https://www.gov.uk/government/speeches/home-secretary-publication-of-draft-investigatory-powers-bill

9 As a country, we have previously disavowed certain techniques - torture[971] and the military targeting of civilians. The Bill contains solely the Home Office and Agency considerations of what they should be allowed to collect: anything they wish, as long as the Secretary of State signs a warrant. Is that sufficient?

Cyber-Security

10 "Cyber-Security", including data, is a tier-one risk identified in the recent Strategic Defence and Security Review, concluding that "Cyber risks underpin many of the other risks we face"[972], with networks forming "an increasingly interconnected world".[973] The UK will not be alone in making such an assessment, with increased digitisation of everything being an opportunity that comes with increased threats. Threats exacerbated by this Bill.

11 The UK wishes to be at the forefront of "big data", especially in healthcare, resulting in the Turing Institute (and the reference to it in the SDSR), and other initiatives. Absent multi-layered protections against other countries agencies doing to UK citizens what we do to theirs, the short term dash to bulk personal datasets throughout government now may have negative long term consequences. Section 5C of the SDSR covered "rules-based international order", yet there is no beginning to creating such an order around bulk personal datasets on civilians.

12 That lack of a rules-based international order is not within the remit or interest of the Home Office, but given the Home Secretary's desire for a "world-leading" regime, it should certainly be of interest to Parliament and all citizens. Where we lead, others will follow. It is UK citizens at disproportionate risk because of the short-sighted recklessness of these powers.

Committee Question: Is the use of bulk personal datasets by the security and intelligence services appropriate?

13 There is no clarity on the *use* of bulk personal datasets by the security and the intelligence agencies. There is only a description that they may be collected, and kept for as long as the agencies believe they may be useful, and that they be used as warranted. Some of the communications Parts of the Bill discuss use, and completely ignore collection.[974] This Part of the Bill solely addresses collection and does not address use. This inconsistency should be addressed.

14 Should our democracy allow our agencies to use data on *"political views, medical condition[s], sexual orientation, or any legally privileged, journalistic or otherwise confidential information"* ? The Home Secretary has asserted that this bill is "not mass-

[971] https://www.liberty-human-rights.org.uk/human-rights/what-are-human-rights/human-rights-act/ article-3- no-torture-inhuman-or-degrading
[972] SDSR, Annex A, paragraph 4: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf
[973] SDSR 6.10 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf
[974] https://twitter.com/richietynan/status/672118838432002049

surveillance", whereas a Peer has elsewhere described it as "blanket surveillance". What characterisation would the Home Secretary use for collecting such data on the "majority of people who are not of security or intelligence interest"?

Data on people who are deceased

15 Clause 150(3) of the draft Investigatory Powers Bill, seeming superficially for entirely practical reasons, treats the data of people who are deceased identically to those who are alive - the Data Protection Act allows them to be treated differently. Given the work of the Agencies, this clause may have unintended side-effects, regarding the ability to access information on individuals who have died, possibly as the result of Agency involvement.

16 All implications of this clause should be carefully considered.

Committee Question: Are the safeguards sufficient for the retention and access of potentially highly sensitive data?

17. The Bill contains discussion of very few safeguards. When compared to those in the ISC report the "safeguards" have simply been harmonised across the agencies. his is better than it was in March when there was no requirement for the Home Secretary to be aware of what the agencies were doing around collecting data on the UK population, and how it can be used. That is still far from sufficient.

18. The bill gives the agencies power to take any data they wish, without a review on usage. The safeguards for that are insufficient. The principle of this power has never even been publicly discussed.

19. Does the Home Secretary have a copy of the nation's medical records, or mental health records, because they feel it "necessary and proportionate" for any purpose? Once the Agencies have the records for one purpose, they may keep indefinitely, and share to others internationally, for any other purpose.[975]

"Disapplies any Duty of Confidence"

20. Paragraph 3.1.6 of the Arrangements[976] "confirms that 'any person' may disclose information to the Agencies for the exercise of their respective functions, and *disapplies any duty of confidence (or any other restriction, however imposed)* which might otherwise prevent this. It further confirms that *information obtained by any of the Intelligence Services in connection with the exercise of any of its functions may be used by that Service in connection with the exercise of any of its other functions.*" (emphasis added)

[975] 3.1.6 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473782/Handling_arrangements_for_Bulk_Personal_Datasets.pdf
[976] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473782/Handling_arrangements_for_Bulk_Personal_Datasets.pdf

21. If the Home Secretary believes this is "an approach that sets new standards for openness, transparency and oversight" it is to be expected that other countries will do what we do. Given the Government's desire to "make England a leading digital health economy in the world",[977] on what basis will other countries not take the same actions against the NHS, as we would take against their health systems?

22. In the same way that UK Armed Forces don't target civilians, our Agencies shouldn't do so digitally, and shouldn't indiscriminately grab British medical records in bulk for any purpose.

23. Once data is available to the Agencies, they can reuse and share it for their other purposes,[978] including purposes that are joint with other organisations. Taken together, this allows GCHQ to use access given for the defence of Critical National Infrastructure, and reuse that data for other purposes with other cooperating Agencies. Given the contents of NHS systems, these powers appear to be the GCHQ poacher moonlighting as a gamekeeper, treating every citizen of the UK as a pheasant.

The need for regular Parliamentary Re-Approval

24. Section 5C of the SDSR covered "rules-based international order", yet there is no beginning to creating such a rules-based international order around bulk personal datasets on civilians. When one is created, we doubt it will look like this Home Office proposal.

25. As the world becomes more digital, the prohibitions discussed here will need review, and reasserting by Parliament. Following the precedent of legislation around the use of terrorism powers around UK citizens, to continue in force, Part 7 of the Bill should be subject to regular affirmative resolution of both Houses, having been preceded by a statement by the Secretary of State making a statement of the kind in para 163(ii), p58, of the ISC report, which covers the types of data held, and disavows the data that is not and and will not be held.

26. The rulings of the Investigatory Powers Tribunal have held that public avowal is all that makes the use of these powers legal. Parliament must maintain this principle, otherwise the situation will degrade to the state which prompted the Snowden revelations that began this whole process.

27. In the 1990s, the availability of terrorism legislation for use against the British public required an annual vote of Parliament. It would be perverse to expect no ongoing scrutiny of Bulk Personal Datasets on UK citizens.

28. These are currently Agency-led arrangements, falling short of the Home Secretary's desire for "world-leading" arrangements. In the first comment Parliament was able to make on the topic, it publicly avowed the details as they currently stood. It appears the

[977] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/384650/NIB_Report.pdf
[978] paragraph 3.1.6 of the Arrangements https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473782/Handling_arrangements_for_Bulk_Personal_Datasets.pdf

Government wishes this to be the only comment Parliament makes. It is up to this Joint Committee of Parliament as to whether you agree.

Explicit clarifications needed on specific points:

29. Is clause 151 parts 1-3, and clauses 152, 153, 154 the complete repeal of any other powers for the collection of bulk personal datasets, other than this Part of the Bill? Are there any other powers under which the agencies will be permitted to collect personal data in bulk?

30. Clause 166. How many warrants are signed by the Secretary of State vs an Official? Will percentages be published by the Investigatory Powers Commissioner in their annual reports? There would seem to be a loophole which allows the civil and diplomatic services to take the load off the Secretary of State. If the Home Secretary wishes to ensure she is personally responsible for signing the warrants, she, and her chain of successors, needs to actually be seen to do the work.

31. Can a communications dataset potentially covered under Parts 4 or 6 of the Bill also be considered Bulk Personal Dataset under Part 7?

6 December 2015

Media Lawyers Association—written evidence (IPB0010)

This is a response to the call for written submissions by the Joint Committee on the draft Investigatory Powers Bill. It is submitted on behalf of the Media Lawyers Association (the "MLA"), which is an association of in-house media lawyers from many of the United Kingdom's leading newspapers, magazines, book publishers, broadcasters and news agencies. A full list of the MLA's members can be made available on request.

Executive summary

The Bill raises a number of significant human rights issues. However, of immediate concern to the MLA, is that the draft Investigatory Powers Bill (the "Bill") as currently drafted provides insufficient safeguards for journalism, and in particular lacks proper protection for confidential journalistic sources and journalistic material. Any order requiring any sort of journalistic material to be handed over to the state engages the right to freedom of expression of publishers and broadcasters under Article 10 European Convention on Human Rights (ECHR) and will amount to an interference for the purposes of Article 10. The Bill provides an opportunity for the UK to send out a modern, strong and robust message about the importance of proportionality and necessity when dealing with journalistic material. The Bill needs better, more comprehensive and stronger safeguards for journalism and journalistic sources, under all the parts of the Bill, not only interception of communications data, but also for example equipment interference and content. Safeguards should also be included to cover related powers of examination of any material obtained and where material is retained for further disclosure and use.

Jurisprudence

Protecting the public from genuine threats to security and safeguarding fundamental rights involves a delicate balance. At the same time, digital developments have produced technological innovations which have facilitated large-scale communications data collection, retention, access and monitoring – which can easily be abused. Widespread violations of these rights have been occurring without appropriate political or judicial oversight. Transparency and proper scrutiny and oversight of such activities are key, even more so where they touch on or involve the Article 10 ECHR rights of journalists.

The press has long been accorded the broadest scope of protection in the European Court of Human Rights's case law, including with regard to confidentiality of journalistic sources. The Court has repeatedly emphasised that Article 10 safeguards not only the substance and contents of information and ideas, but also the means of transmitting it. There has been a long line of cases in Strasbourg setting out that source protection is a key part of the Article 10, from *Goodwin v UK* in 1996, through to *Sanoma v. The Netherlands* in 2010, *Telegraaf Media Nederland Landelijke Media B.V. v. The Netherlands* in 2012 and *Nagla v. Latvia* in 2013.

Any order requiring journalistic material to be handed over to the state engages the right to freedom of expression of publishers and broadcasters under Article 10 ECHR and will amount to an interference for the purposes of Article 10.1 (see eg *Handyside v United*

Kingdom (1976) 1 EHRR 737 at paras 14 and 43 and *Tillack v Belgium* (App No 20477/05 27 November 2007). The right to a fair hearing (Article 6 ECHR) is also engaged by such applications, emphasising the crucial importance of the media being given the opportunity to make informed representations at an *inter partes* hearing before their material is accessed or obtained.

The need for protection of journalistic sources has also been widely recognised by other international bodies, including the European Parliament, the European Court of Justice3, the Committee of Ministers of the Council of Europe, the IACMHR and the ACHPR. The OSCE member states stated, in the Concluding Document of their 1986-1989 Vienna Follow-Up Meeting: "[J]ournalists ... are free to seek access to and maintain contacts with, public and private sources of information and that their need for professional confidentiality is respected." Such fundamental right must be properly safeguarded in order that they can be effectively exercised.

The Council of Europe Recommendation No R (2000) 7 of the Committee of Ministers on the right of journalists not to disclose their sources of information makes clear that "source protection" applies not just to the identity of the source but to all matters relating to and communications with the source. This includes not just the name and personal data as well as the voice and image of a source, but the factual circumstances of acquiring information from a source by a journalist, including the unpublished content of the information provided by a source to a journalist.

The importance of protecting sources

If sources think they can be identified they will be reluctant to pass on information or to take the risk of disclosure, dismissal (or possibly prosecution). Without proper protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public-watchdog role of the press may be undermined and the ability of the press to provide accurate and reliable information may be adversely affected. The public will get fewer stories telling them things that government and big business does not want them to know. Journalists will be lessened in their ability to hold the powerful to account and to shine a light on corruption and crime.

"Protection of journalistic sources is one of the basic conditions for press freedom. ... Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public-watchdog role of the press may be undermined, and the ability of the press to provide accurate and reliable information be adversely affected. ... [A]n order of source disclosure ... cannot be compatible with Article 10 of the Convention unless it is justified by an overriding requirement in the public interest." (*Goodwin v. the United Kingdom,* judgment of 27 March 1996, § 39)

Journalists routinely deal with their sources on their mobile phones and laptops. As has been shown by the use of RIPA to obtain details of calls made by the Sun's Tom Newton Dunn to his sources, covert access by State authorities has become a quick and easy way to identify a source, bypassing the protections enshrined in the Police and Criminal Evidence Act 1984. The loopholes in the Regulation of Investigatory Powers Act 2000 (RIPA) exposed by the Tom

Newton Dunn case are still not adequately dealt with.

Existing protection under the Police and Criminal Evidence Act 1984 (PACE) and the Terrorism Act 2000.

Under PACE a distinction is made between journalistic material and confidential (i.e. source) journalistic material ("excluded material"). Journalistic material is material acquired or created for the purposes of journalism. This definition is very broad and covers everything from a journalist's own notes to unpublished film footage, sound recordings, photographs and documents provided to journalists by their sources as well as the identity of the source. Where journalistic material is concerned, under PACE it is necessary to provide sufficient information to the media to enable them to be satisfied that, on the face of it, certain access conditions have been met, which include:

- Details of the offence that it is believed has been committed or in general terms the investigation to which it relates;
- the material that is sought;
- why the material is believed to be likely to be of substantial value (whether by itself or together with other material) to the investigation in connection with which the application is made;
- what other methods of obtaining the material have been tried - the journalist should be the last, rather than the first, means of arriving at evidence required;
- why it is believed to be in the public interest that the material should be produced or that access to it should be given.

If excluded material is sought there are a higher set of access conditions that have to be met, which are essentially that prior to the enactment of PACE, access could have been gained to the material under a search warrant. There are very few, rather obscure, enactments that fall under this category, including s.19(3) Wildlife and Countryside Act 1981, s.15 Wireless Telegraphy Act 1949 and s.4 Biological Weapons Act 1974. Accordingly, applications for excluded material under PACE are rare. It is permissible, however, to gain access to excluded material under the provisions of the Terrorism Act 2000, provided that the material is sought for the purposes of a terrorism investigation, the officer has reasonable grounds to believe that the material will be of substantial value, and the officer has reasonable grounds for believing that the material should be produced.

The state cannot therefore obtain any journalists' information – whether confidential or not - unless there is an overriding public interest requiring disclosure. This is a balancing exercise but one where the public interest in protecting journalistic sources is accorded proper weight. Such applications must normally be heard by a Judge, on notice, so that the judge has the benefit of evidence and argument from the journalist as well as the state. These considerations mean that covert access should only be used to identify sources in the most exceptional cases.

Recent problems – unlawful use of RIPA

Part I of RIPA deals with the interception, acquisition and disclosure of communications data. Part II deals with covert and human surveillance. Since September last year, several cases of police forces using Part 1 of RIPA to find journalistic sources have emerged. Last year, Cleveland Police emerged as the fifth force to have used RIPA to obtain journalistic phone records to identify a source. The first case of a police force secretly obtaining journalistic phone records to find sources emerged in September 2014, when, the Metropolitan Police admitted to obtaining Sun phone records to find the source of its Plebgate story. Subsequently, it was revealed that the Kent/ Essex, Suffolk and Thames Valley forces had used RIPA in similar circumstances. Earlier this month, the Interception of Communications Commissioner, Sir Stanley Burnton found that Scottish police had breached the most recent set of rules by failing to gain judicial approval for five applications for communications data, which aimed either to find a journalist's source or obtain the communications of those suspected of having acted as intermediaries between a journalist and a suspected source[979]. He was also satisfied that the applications failed to satisfy the requirements of necessity and proportionality, or to give due consideration to Articles 8 or 10 of the European Convention on Human Rights. In addition, a Designated Person (DP) who was not independent of the investigation approved two of the applications. These failings were breaches of RIPA Acquisition and Disclosure of Communications Data Code of Practice 2015, which came into force on March 25 this year, and required police forces to obtain judicial approval before obtaining journalistic records in this way.

The Interception of Communications Commissioner's Office ("IOCCO") held an investigation into police use of RIPA to find journalistic sources at the end of last year. When published in February, it revealed that 19 forces had used RIPA in this way to obtain the records of 82 journalists over a three-year period. Overall, there were 105 journalists at the centre of leak investigations reported to IOCCO, with 78 per cent having their own records obtained. Some 19 of the 105 were listed as working in the local/ regional press.

In 2008, the Chief Constable of Thames Valley Police granted authorisation under Part II RIPA (which deals with covert and human surveillance) for his officers to place a probe inside the car of one of their officers, who they suspected of being a source for a journalist called Sally Murrer, who worked for the Milton Keynes Citizen. This enabled his discussions with Ms Murrer to be recorded. On the back of these recordings, the police arrested Ms Murrer and strip-searched her. They searched both her home and her desk area in the newsroom. They subjected her to an interview in which it was suggested that she had paid the source (an allegation which was untrue and unsupported by any evidence) and that she could go to prison for what she had done. She was charged with aiding and abetting misconduct in public office – being the alleged misconduct of the officer said to have disclosed information to her. Once prosecuted, she was entitled to disclosure of all the police records of the investigation. These included the papers relating to the Chief Constable's authorisation and the approval of the authorisation by a Surveillance Commissioner (a retired judge). These papers made no reference to the fact that Sally was a journalist or that the investigating officers were seeking to identify a confidential journalistic source. The prosecution was eventually halted by an order of the Kingston Crown Court – which recognised that this key evidence against Ms Murrer and the officer had been obtained in violation of fundamental

[979] http://www.iocco-uk.info/docs/Press%20statement%2025-11-2015.pdf

journalistic rights[980].

Problems with the draft Bill as far as journalistic source material is concerned.

While it is to be acknowledged that the Bill (unlike RIPA) includes new protections which give explicit protection to journalists, in addition to the fact that the problems exposed for example by the Sally Murrer case with regard to misuse by authorities of covert surveillance powers under Part II of RIPA remain, the new protections do not go far enough: the Bill creates a route whereby the state can identify a source without going thorough the PACE protections. Further, the clause in which the limited protections provided appear (clause 61 of the Bill) is in the part of the Bill which deals only with communications data, there are no specific protections included anywhere else in the Bill for any of the other wide ranging powers of collection and retention.

Clause 61 requires that police forces must get the approval of an independent "Judicial Commissioner" before accessing a journalist's communications data (the service provider's record of who they phoned, texted or emailed, from where and when, from which their sources can then be identified) in order to identify a source.

This so called double-lock procedure, which is linked to proposed Codes which would apply to communications data, interception and equipment interference, is simply not strong enough: Codes have previously been ignored, so it is vital that fundamental protections such as these are included in the primary legislation. All safeguards ought also to apply to the RIPA part 11 (ss 26-46) powers of intrusive and covert surveillance that have also been deployed against regional journalists to discover sources. The safeguards ought to be equivalent to the PACE procedure and should require applicants' mandatory disclosure to the Home Secretary and / or Judge that the subject of the application might include information that could relate to media organisations, journalists and their sources and that purpose, or whether the direct or indirect effect of the power applied for may involve the identification of confidential sources.

The Bill does not contain a sufficiently wide definition of journalistic material.

Most worryingly, applications to the Judicial Commissioner can be made without the knowledge of the media organisation concerned. The Bill contains no right to prior notification, nor the right to contest an application before a judge, *before* the investigatory power is granted. And while the applicant can challenge a refusal, there is no scope for media contest or challenge. The judge will only have the police's side of the case, as the journalist will not be told anything. The case for protecting press freedom will not be articulated. These are all procedural safeguards that have been recognised by the ECtHR as essential for source protection.

Further, there is a concern about the regime proposed (whereby the Judicial Commissioner is to apply 'the principles of judicial review' to Ministerial consent to communications data being obtained). While this suggest a judge will at least have to assess whether the police

[980] https://inforrm.wordpress.com/2014/11/14/journalistic-freedom-ripa-and-misconduct-in-public-office-lessons-from-sally-murrers-case-gavin-millar-qc/

have “reasonable grounds” for the intrusion, it appears to be only a *review* of a police decision, already taken, against a lower standard than is required under PACE: the judge does not make the decision.

This judicial oversight procedure does not in any event cover applications by the intelligence services.

Urgency procedures allow this ‘so called double lock’ to be bypassed, even where it applies, so that the powers can be used and damage done long before the review deadline and any possible revocation.

There is no reference or acknowledgment in the Bill to a right of source protection that can only be displaced by an overriding public interest. Nor must the police exhaust other lines of inquiry. The data can be obtained for any number of reasons, including investigation of any crime, however minor.
The police and others will still therefore be able to evade the tougher PACE requirements by using these alternative powers in much the same way as they have been using RIPA.

Other specific concerns relating to clause 61 / source protection

1. The Bill will make the requirement for applications to access the communications data to be authorised by a Judicial Commissioner only where it is for the specific “purpose of identifying or confirming the identity of a journalist’s source”. It is often the case that identifying a source is collateral or incidental and safeguards need to be in place for those occasions. The judicial oversight only applies if the purpose of the application is to identify a source. I.e. if the investigating authority argues that the application is for some other purpose, it is irrelevant if a source is identified in the process. There is no judicial oversight of data collection involving journalists or journalism if the purpose of the application is for any other reason than identifying a source or where obtaining the identity of a source may not be the primary purpose but there is a risk or likelihood that the source may incidentally be identified. Here, the Bill should follow the Strasbourg approach on the gathering of what turns out to be legally privileged material – viz when it is reviewed and seen to have source identifying potential, you stop and bring in the independent quasi-judicial assessor to look at the material in the context of the investigation. She then applies the Goodwin principles to decide not whether you can use the intrusive technique but whether you can use the material any further in the investigation.

2. There is nothing as to what happens should data which accidentally identifies a source is obtained.

3. The Definition of journalistic material in the draft Bill is very narrow. Clause 61 (7)) says that “source of journalistic information” means “an individual who provides material intending the recipient to use it for the purposes of journalism or knowing that it is likely to be so used.” The clause only deals with source related information. The purpose of journalism is not defined.

This definition is much narrower than the equivalent provision in s 13 PACE, which defines "journalistic material" as "material acquired or created for the purposes of journalism". Further, section 13 PACE continues "(2) Material is only journalistic material for the purposes of this Act if it is in the possession of a person who acquired or created it for the purposes of journalism. (3)A person who receives material from someone who intends that the recipient shall use it for the purposes of journalism is to be taken to have acquired it for those purposes." Under the draft clause it is not clear for example that information acquired by a journalist for the purposes of a sensitive journalistic investigation, not yet published, would be protected.

4. The Bill also contains problematic proposals for investigative journalism and protection of sources on "equipment interference" - the capability for security services and the police to remotely hack technology. This permits, for example, the police to access a smart phone and use its microphone covertly to record sound, without the knowledge of the owner. This was already being done by the security services, but the parameters will now be defined in statute. A judicial warrant will be necessary, and a code of practice will be brought in to regulate "the use of more sensitive and intrusive techniques."

5. The blanket retention of 12 months' of records of all websites visited by British citizens, referred to by the Home Secretary as "simply the modern equivalent of an itemised phone bill", would help identify the object and progress of journalistic investigations by individuals or teams. Authorities would have to use the same application process as for communications data.

Attached as Appendix 1 below is a draft-revised clause 61, which it is submitted would comply with the Strasbourg principles on source protection.

Problems with the draft Bill as far as other journalistic material is concerned

The only area where the Bill attempts to address concerns about the protection of journalistic sources and the media's right to freedom of expression is in clause 61. Clause 61 is in the part of the Bill that deals only with communications data - there is nothing in the Bill dealing with the position regarding seeking content which does not identify a source. It therefore leaves it unclear as to what, if any, is the appropriate route where the police or the intelligence services want to obtain or access journalistic content (for example unpublished pictures from a riot).

Clause 61 only deals with sources, but doesn't deal with more general journalistic material - for example unpublished material [which is covered under PACE, albeit with a lower set of thresholds than for source material]. Article 10 doesn't just cover source issues, it covers speech protection much more widely. Strasbourg only sets minimum standards and domestic law can be more protective of journalistic free expression, though not less.

So the Bill also needs to cover content related issues around obtaining more general journalistic material. There is therefore a need to construct either a workable and clear regime for protecting content which is unpublished/confidential or clarify that all

applications to obtain such material should be dealt with under the existing procedure in PACE . Any provision relating to this needs to appear in a different part of the Bill from clause 61.

Further, as indicated, other RIPA powers and investigatory powers have been used against journalists and media organisations, so this Bill provides a real opportunity to suggest more comprehensive and clear safeguards in this area as well.

Conclusion

The Bill does not adequately protect journalistic material. It does not comply with the basic Strasbourg safeguards recognised under Article 10. It is too narrowly drafted and requires amendment to give the appropriate and necessary protections for journalistic material and sources. These should mirror the procedural and substantive safeguards contained in PACE.

Appendix 1 - Proposed new Clause 61

Special procedure for obtaining information identifying a journalistic source

1. There is a public interest in the protection of journalistic sources and journalists have a right not to disclose information identifying a source.
2. The powers identified in sections 46 - 60 may not be used to obtain communications data if the effect of using the powers (under sections 46 - 60) is to obtain information either identifying a source or which could contribute to identifying a source.
3. A relevant public authority may only obtain communications data for the purpose identified in sub-section (2) by making an *inter partes* application to a circuit judge.
4. The respondent to the *inter partes* application under sub-section (3) is the journalist whose communications data is being sought, and any employer of that journalist.
5. Paragraphs 7 – 9 of the Police and Criminal Evidence Act 1984 shall apply in relation to the service of a notice of application for an order under sub-section (8) below as if the application were for an order under Schedule 1 Police and Criminal Evidence Act 1984.
6. If on an application under this section the circuit judge is satisfied that conditions specified at sub-section (7) below have been met, the circuit judge may make an order under sub-section (8) below.
7. A circuit judge may only make an order under sub-section (8) if the public authority has convincingly established that:

a) the order is directed to one or more of the legitimate aims specified in Article 10.2 of the Convention, and
b) there is an overriding public interest which makes it necessary for the public authority to obtain the communications data in issue notwithstanding the public interest in non-disclosure and the right of the respondent not to disclose information identifying a source, and
c) reasonable alternative measures to the disclosure do not exist or have been exhausted by the public authority, and
d) the order is proportionate to the legitimate aim or aims being pursued.

8. An order under this sub-section is an order requiring a telecommunications operator or other person in possession of specified communication data which is in existence to disclose it to a specified person.

9. In this Act:

a) “journalist" includes any natural or legal person who is regularly or professionally engaged in the collection and dissemination of information to the public via any means of mass communication;

b) "information" means any statement of fact, opinion or idea in the form of text, sound and/or picture, whether in digital or other form;

c) "source" means any person who provides information to a journalist;

d) "information identifying a source" means:

i) the name and personal data as well as voice and image of a source;
ii) the factual circumstances of acquiring information from a source by a journalist;
iii) the unpublished content of the information provided by a source to a journalist;
iv) personal data of journalists and their employers related to their professional work; in so far as this is likely to lead to the identification of a source.

e) “the Convention” means the European Convention for the Protection of Human Rights and Fundamental Freedoms

11 December 2015

Mental Welfare Commission for Scotland—written evidence (IPB0029)

1. The Mental Welfare Commission is a statutory body, with powers under the Mental Health (Care and Treatment) (Scotland) Act 2003 and Adults with Incapacity (Scotland) Act 2000 to protect and promote the human rights of people with mental health problems, learning disabilities, and related conditions. This includes powers to oversee the operation of security measures in relation to detained patients.

2. Our submission relates to clause 38 of the Investigatory Powers Bill. In relation to Scotland, it authorises 'interception' in the State Hospital (Scotland's high security psychiatric hospital) if it is conduct in pursuance of, and in accordance with, any direction given to the State Hospitals Board for Scotland under section 2(5) of the National Health Service (Scotland) Act 1978.

3. We are concerned that this does not properly take account of the statutory framework within which security measures, including interception of postal correspondence and telephone calls, operate in Scottish psychiatric hospitals. This is set out in sections 281 to 286 of the Mental Health (Care and Treatment) (Scotland) Act 2003.

4. Sections 281-283 make detailed provision in relation to interference with postal communications. These are supplemented by regulations – the Mental Health (Specified Persons' Correspondence) (Scotland) Regulations2005 (SSI 2005/408). http://www.legislation.gov.uk/ssi/2005/408/made/data.pdf

5. Section 284 provides for regulations on the use of telephones (including interception), and s285 gives a direction-making power to Scottish Ministers as to the implementation by hospital managers of those regulations. (See the Mental Health (Use of Telephones)(Scotland) Regulations 2005 (SSI 2005/468) http://www.legislation.gov.uk/ssi/2005/468/made/data.pdf .

6. As a bare minimum, the Investigatory Powers Bill should make clear that any action which is authorised under the 2003 Act powers is lawful.

7. Furthermore, unless there is some clear justification, the Bill should not add another route to authorising interception in a psychiatric hospital when there is already a statutory regime covering this. That is likely to create confusion as to how the two regimes interact.

8. The approach of the 2003 Act is preferable, as much of the detail is in secondary legislation rather than Ministerial direction, so is subject to a greater degree of Parliamentary scrutiny. If there is concern that there are gaps in the framework of the 2003 Act, these gaps should be addressed within that framework, rather than create two overlapping regimes.

17 December 2015

Dr. Glyn Moody—written evidence (IPB0057)

My name is Glyn Moody. I am a journalist, and have been writing about computers, the Internet and surveillance for print and online publications including The Economist, Financial Times, The Guardian, The Telegraph and many others, for over 30 years. I have two degrees in mathematics from Cambridge University, which is of some relevance for technical areas such as encryption. I am making this submission in a personal capacity.

1. The proposed powers are not necessary, because they are predicated on an erroneous idea: that mass surveillance works. There is no evidence that is does, and evidence that it does not - see http://arstechnica.co.uk/tech-policy/2015/11/terrorist-attacks-mass-surveillance-is-the-problem-not-the-solution/. This notes that the vast majority of terrorists involved in recent attacks were known to the authorities; the problem was not finding them, but allocating resources to deal with them. Mass surveillance makes things worse by throwing up false positives, and those, in turn, cause resources to be wasted. As an FBI whistle-blower with experience of mass surveillance and its failures put it: "If you're looking for a needle in a haystack, how does it help to add hay?" - http://www.theguardian.com/commentisfree/2014/nov/28/bigger-haystack-harder-terrorist-communication-future-attacks.

2. The proposed powers are almost certainly not legal. The CJEU Digital Rights Ireland judgment makes it clear that indiscriminate mass surveillance breaches human rights. The more recent case of Roman Zakharov v. Russia at the European Court of Human Rights similarly found that indiscriminate mass surveillance was unacceptable. It seems likely that the Investigatory Powers Bill would be ruled a violation of basic human rights in multiple fora.

3. The proposed powers are not workable because they are based on fundamental misunderstandings of how the Internet works today. In particular, the idea of an Internet Connection Record is almost completely meaningless - more details here: http://arstechnica.co.uk/tech-policy/2015/11/uk-isp-boss-points-out-massive-technical-flaws-in-investigatory-powers-bill/. The infeasible nature of the plans has been confirmed recently by the UK's main telecoms companies – http://arstechnica.co.uk/tech-policy/2015/12/snoopers-charter-so-technically-complex-that-it-may-be-infeasible-telcos-say/. Trying to build systems that can store these mythical Internet Connection Records will inevitably produce another IT implementation fiasco that has sadly made UK projects, especially those in government, a by-word for failure throughout the world.

4. As has been widely observed, the authorisation system does not provide a "double-lock", because the judicial review is only of whether the first authorisation process was carried out correctly, not whether the authorisation was justified. As such, it lends no credibility to the procedure. Full, independent judicial authorisation on a case-by-case basis is the only way for the system to be just and perceived as such. Absent that independent judicial element, it must be regarded as a purely political process ripe for abuse.

5. The distinction between "content" and "communications data" is meaningless, and again betrays an ignorance of how modern digital systems work. "Communications data" is

metadata; the only difference between metadata and data is that metadata is pre-sorted into conceptual categories – sender, date, location, email address etc. - while content is unsorted. As such, metadata is hugely more valuable than content, because it can instantly be combined with other metadata; indeed, the power of computers today is such that it can be combined with billions of other metadata elements. Content, by contrast, is largely useless for this purpose, because computers cannot understand it. Before it can be used, it must be parsed – texts must be "read", images "seen." Currently, those are very hard computing tasks; that means content is not useful for scalable analysis (although it is valuable for human-based scrutiny, but does not scale.) So the idea that "communications data" is somehow less intrusive than gathering content is not just wrong, but exactly wrong: it is hugely more intrusive, which is why it should never be gathered routinely, as proposed here.

6. Not only is the retention of data obtained through mass surveillance likely to fail legal challenges, it will also – inevitably – be obtained by criminals and/or state actors if it is held in databases. If they are ever built, they will create targets that will be irresistible to thieves and foreign intelligence services. It is impossible to secure dozens of these new databases in the long term: some will always be broken into, either through skill, bribery, blackmail or luck. As noted above, metadata is the most revealing of all data, so the huge metadata stores held in these databases will be precisely the most valuable for identity thieves and for foreign governments wishing to profile and perhaps blackmail UK citizens. Creating digital honeypots in this way is beyond foolish.

7. The whole idea of "equipment interference" is short-sighted in the extreme. Undermining the security of any part of the digital ecosystem undermines that ecosystem as a whole. That is particularly true of encryption: happily, the idea of weakening encryption or adding backdoors is now so discredited that nobody with any understanding of the topic would even suggest it. But there is another aspect that has not been discussed. If "equipment interference" is permitted, it will ultimately harm the entire UK legal system. That may seem an unlikely outcome, but if "equipment interference" becomes widely practised it is only a matter of time before court cases are dropped because the evidence presented cannot be relied upon. If it is permitted to put anything on anyone's machine – and technically, that is quite possible – then the evidence found on computers cannot be trusted: incriminating files can be loaded, browsing histories edited to show suspicious patterns of use or visits to illegal sites, etc. Allowing "equipment interference" may sound like a clever technical approach for surveillance, but the collateral damage to society will be huge as computer-based evidence becomes increasingly central to court cases.

Glyn Moody

London

19 December 2015

Ms Susan Morgan—written evidence (IPB0043)

1. Until mid December 2014 I was Executive Director of the Global Network Initiative (www.globalnetworkinitiative), a Washington DC based multi-stakeholder initiative focused on the responsibility of technology companies to protect the privacy and free expression rights of their users around the world. I previously spent a decade at British Telecom. The views below are my personal perspective based on fifteen years working in and around the technology industry and on these issues.

2. The introduction of legislation to consolidate the myriad existing legislation and bring greater clarity and transparency is to be welcomed.

3. It is disappointing to see that the amount of time available for the committee to scrutinize the bill has been reduced. This reduced time for scrutiny means that greater reliance should be placed on the recommendations in the David Anderson and RUSI reports and the Sheinwald review published earlier this year.

4. Whilst I welcome the introduction of the legislation, it is difficult to avoid the conclusion that parts of the bill are designed to put on a firmer footing some of the programmes revealed by Edward Snowden and the very broad interpretation of existing legislation used to provide the legal basis for these activities. Given this, my own reading of one of the things the bill needs to achieve is to restore trust that has been lost. This is underlined by the avowal in Parliament during the introduction of the bill that section 94 of the Telecommunications Act 1984 had been used for the bulk collection of communications data. In my view the bill as currently drafted does not meet this test. Specific recommendations on what could be done to better meet this objective are set out below.

5. As the legislation is scrutinized, consideration must be given to the important role the UK government has in setting standards around the world. It is essential we do not legislate in isolation. We must seriously consider the international signal we will be sending and whether we would be comfortable to see less democratic nations using our legislation to justify their own actions. The UK's role as a founding member of the Freedom Online Coalition (https://www.freedomonlinecoalition.com/), a coalition of 29 governments dedicated to advancing Internet freedom is particularly important in this regard.

6. Relating to the previous point, the UK must also consider the precedent setting issue with regard to the extra-territoriality provisions in the bill. It is reasonable to assume that other governments could replicate these aspects of the bill which is likely to impact British companies operating overseas and put UK technology users at risk. The clear direction of travel in both the Anderson report and the Sheinwald review is on the importance of additional international agreements and cooperation where necessary. In the United States Congress has already granted the Department of Justice additional funds for Mutual Legal Assistance Treaty reform. Many of the major powers in this bill unilaterally impose extra-territoriality. Serious consideration

must be given to whether this is the intention of the bill and the potential consequences to this.

7. This bill could regulate the critical relationship between citizen and state for many years. The bill is a long and complex one and with many definitions within it that could be subject to potentially broad interpretation. As a matter of principle as much as possible should be in the primary legislation. But in the case that additional codes or statutory instruments will be produced the committee should consider requesting that they are issued now. If this isn't possible, as a minimum they should be published at the same time as the bill to enable scrutiny in Parliament. This would reduce the potential for misinterpretations when the bill is enacted and presumably also enable more precise costs to be determined. It is important at a time of tight government finances, particularly if the tax-payer is to fund these activities through a cost recovery model for the tech companies that will have responsibility for meeting government requests.

8. A key recommendation in the Anderson report was that the bill should be understandable to a layperson. Arguably in its current form the bill fails this test. The bill must be scrutinised with this in mind.

9. On the bulk collection of data, it is very important to note the different direction the UK is taking compared to both the US and the direction of travel in reports over the last couple of years at the UN Human Rights Council (HRC). The US Freedom Act passed in June 2015 for the first time since 9/11 reduced the scope for bulk collection of data. This sharply contrasts with the provisions for the introduction of the retention of Internet Connection Records. Several reports that have been presented to the HRC since 2013 have raised serious reservations about the collection of bulk data and mass surveillance. If not already, I would urge the members of the scrutiny committee become familiar with the following reports and consider the Investigatory Powers Bill in this context:

    a. April 2013 – Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression – Frank La Rue http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

    b. 30 June 2014 – The Right to Privacy in the Digital Age – Report of the Office of the United High Commissioner for Human Rights http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

10. Regarding the issue of judicial authorisation, it seems to me that the current partial introduction (with the review limited to that of a process review rather than an independent evaluation of the facts by the judiciary) is wholly inadequate given the very broad range of powers included in the bill. For example, at the very least provisions in the bill for equipment interference (or legalised hacking) are very controversial and create a compelling case for a full independent evaluation of the

facts by the judiciary as well as a process review. The recommendations from the Anderson report should be accepted in full.

11. On encryption, the bill is not convincing on two issues. It doesn't address the reality that there are ways around the provisions for those determined that their communications will be beyond the reach of the government. And secondly, it doesn't address the reality that encryption is an essential part of making the Internet safe for the many activities people undertake online. Actions to undermine encryption will necessarily make the Internet less secure. I would urge the committee to consider these two issues carefully and seek specialist advice. The UK has one of the top digital economies in the G20. Security and encryption are a key part of retaining this.

12. Finally, although there is a balance to be struck, to address the issues of trust raised by the Snowden revelations there needs to be an assumption of openness and transparency about the activities the government is undertaking. Disclosure by default should be the standard unless there is an operational reason. The agencies should be required to make the case for secrecy. There is also a direct link between transparency and access to remediation, with users whose privacy may been violated unable to seek remedy if secrecy provisions prevent them being made aware of the potential violation. In areas of the bill where there are gagging clauses (and particularly in the case where companies are prevented from communicating with their customers about what they are being asked to do) as a point of principle I would ensure these clauses have an end point and the case then needs to be remade for information to remain secret.

18 December 2015

Mozilla—written evidence (IPB0099)

Summary

This submission will focus on Mozilla's key areas of concern with the draft Bill which will require careful scrutiny and consideration before it moves forward:

1. About Mozilla

1.1 Mozilla's mission is to promote openness, innovation, and opportunity on the Web. We produce the Firefox Web browser and Firefox OS mobile ecosystem, together adopted by half a billion individual Internet users around the world. Mozilla is also a non-profit foundation that educates and empowers Internet users to be the Web's makers, not just its consumers. To accomplish this, Mozilla functions as a global community of technologists, thinkers, and builders—including many contributors and developers in the United Kingdom—who work together to keep the Internet alive and accessible. We are legally registered in the UK, maintain an office in London, and around 100 of our employees live here. Additionally, every year we bring thousands of people to the Greenwich Peninsula for the Mozilla Festival, a weekend-long celebration of making and building on the Web.

2. Introduction

2.1 The open Internet relies on technological and legal design decisions to ensure its continued vitality. Unfortunately, the legislation before you would undermine that framework, and represents a serious threat to open source software, online commerce, and user privacy, security, and trust. A comprehensive revision of the Investigatory Powers Bill is necessary to protect the Internet and its users.

2.2 The bill proposes a broad and dangerous set of surveillance mandates and authorities that threaten privacy and security online. Keeping Internet users safe does not have to cost

them their privacy, nor the integrity of their communications infrastructure. We believe the current legislation falls far short of striking the right balance.

2.3 As we have previously outlined in our written evidence submitted to the Science and Technology Committee of the House of Commons,[981] we have serious concerns regarding:

- Requirements to undermine encryption that pose a severe threat to trust online and to the effectiveness of the Internet as an engine for our economy and society;
- Bulk equipment interference authorities that could be used to violate the integrity of Internet technologies generally and harm our industry's relationship with our users;
- Limitations on disclosure that impact our open philosophy and in practice are unworkable for an open source company;
- Bulk interception capabilities that would compromise the privacy of communications; and
- Data retention mandates that create unnecessary risk for businesses and users.

2.4 In an effort to better understand the impacts of these broad powers on Mozilla and other organisations, we have engaged in conversations with the Home Office to provide their interpretation of the bill. We very much appreciate and welcome the Home Office's openness and willingness to engage. Yet many of the issues on which we have identified questions remain unresolved, in particular relating to sections 4, 5, and 6 of this filing.

2.5 In the absence of such clarity we are currently unable to fully understand what might be demanded of Mozilla and other technology organisations. We therefore have great concern about the broad scope of this bill and how and to whom these obligations might apply. These concerns are outlined in greater detail in Section 3.

2.6 Mozilla is concerned with the ripple effect this bill would have on the Internet ecosystem. In particular, in proposing such a broad range of powers without precisely defining roles, definitions, and scope, this bill would generate legal uncertainty for businesses operating in the UK, in addition to inflicting great harm to the security of users and Internet infrastructure.

2.7 We strongly encourage the IP Bill Committee to thoroughly scrutinise this bill, and in particular, to weigh the bill's effectiveness and intended objectives with the adverse impacts

[981] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25237.html

it would have on the health and continued success of the Internet economy in the UK and globally.

3. The Bill would create an environment of legal uncertainty for UK business

3.1 It remains unclear whether and to what extent open source software developers such as Mozilla might be impacted by the various provisions of the Investigatory Powers Bill. The powers sought are not workable or carefully defined. Specifically:

- The ambiguous definitions, in particular what constitutes a Communications Service Provider (CSP);
- The broad scope including bulk powers which are permissible outside of the "bulk" provisions;
- Expansive applicability of the powers sought, in particular through the broad definitions of "equipment" and "communications data."

3.2 As the draft bill does not clearly define the how and the what and the who, it risks creating an environment of legal uncertainty which can chill innovation and the health of the Internet economy. Just as the application of these powers is not directly apparent to Mozilla, it is hard to believe that other organisations would have more clarity than we do. Such an environment of legal uncertainty risks creating a chilling effect, particularly for smaller businesses and startups which may not have legal teams or appetite for such risk and might be dissuaded from operating in the UK in the future.

3.3 ***On definitions:***
We don't have clarity on whether and which products and services in particular might fall under the obligations, particularly through the formulation of "Communication Service Providers." No discrete definition of CSPs exists in the text, where a range of definitions can be found in Section 193 on Telecommunications Definitions.[982] As a forward looking organisation, it is also possible that we might one day build a service that might fall under these requirements even assuming that we do not today. For those who are not explicitly telecommunications operators, organisations like Mozilla will be operating in a legal grey zone unless these obligations and roles are further refined.

3.4 ***On scope:***
The scope of the interception and interference capabilities are dangerously expansive. Specifically, the broad powers envisioned through the bulk provisions seem to be permissible outside of the "bulk" provisions. This is particularly evident in the case of "thematic warrants"[983] which can be authorised under the "targeted" interception and equipment interference provisions. Sections 13 and 83 which list the criteria upon which targeted interception and equipment interference warrants may relate to refer to "groups of persons"; "more than one person or organisation, or more than one set of premises";[984] equipment belonging to an "organisation"; "people that form a group"; a "particular location" or "more than one location"; or "for the purposes of a particular activity or

[982]Section 193, Telecommunications Definitions, Investigatory Powers Bill
[983]Explanatory Notes, para. 212, Investigatory Powers Bill
[984]Section 13(2), Part 2, Draft Investigatory Powers Bill

activities of a particular description."[985] It is hard to understand any of the above terms as being "targeted" and not "bulk".

3.5 ***On application:***
In the current form of the Bill, the formulation of "data" (communications data, and the newly proposed events and entity data) is troubling. In particular, the meaning of "data" even includes, "any information which is not data."[986] It also seems as though there will be no device, or piece of data that would not be subject to intrusion. In defining "equipment", it "means equipment producing electromagnetic, acoustic or other emissions or any device capable of being used in connection with such equipment."[987] The Bill would apply not only to mobile phones, tablets, and laptops, but to any electronic device connected to the Internet. With the increased adoption of wearable devices, such as smart watches that monitor heart rate and breathing patterns, such broad scope presents a relative Pandora's Box of bulk collection and intrusion, largely affecting people who are not suspected of and have not committed any wrongdoing.

3.6 These ambiguities must be clearly articulated so individuals have the capacity to understand the extent and tools with which surveillance is being undertaken by their government. Likewise, businesses require an environment of legal certainty within which to operate, particularly if they are offering secure and privacy-preserving products and services; overbreadth of scope prevents such certainty from being possible. In order for this reform to remain within the contours of a workable framework for the Internet economy and the security of users, these definitions and application of powers must be significantly refined.

3.7 The lack of clarity on the definitions, scope, and applicability of the draft Bill has served to exacerbate our concerns outlined below.

4. Obligations to weaken the security of our products

4.1 The draft Bill permits encryption backdoor mandates through the obligations imposed by a "maintenance of capability order," which may include an obligation to "remove the electronic protection applied by a relevant operator to any communications or data."[988] In practice, this provision could be used to force companies to undermine the encryption protecting user communications—for example, for users of Hello, our encrypted in-browser video conferencing service—unacceptably placing their private data at risk. Moreover, the possibility that companies might be forced to weaken encryption on products would erode user trust in those products, harming the continued success of online commerce. This has a potentially huge impact on the Internet: Firefox encrypts 100 billion individual Web data transfers for our users every day.

4.2 Requirements that systems be modified to enable government access to encrypted data are a threat to users' security. The primary aim of computer security is to protect user data against any access not authorised by the user; allowing law enforcement access violates that

[985]Section 83, Part 5, Draft Investigatory Powers Bill
[986]Section 195, General Definitions, Draft Investigatory Powers Bill
[987]Section 105, Part 5: Interpretation, Draft Investigatory Powers Bill
[988] Section 189(4)(c), Maintenance of technical capability, Chapter 1, Part 9, Investigatory Powers Bill

design requirement and makes the system inherently weaker against the attacks that it is intended to defend against. Once systems are modified to enable law enforcement access by one government, vendors will be under enormous pressure to provide access to other governments. It will not be possible in practice to restrict access to only "friendly" actors. Moreover, the more government actors have access to monitoring capabilities, the greater the risk that non-governmental cyberattackers will obtain access. Endpoint law enforcement access requirements are also incompatible with Open Source and open systems because they conflict with users' right to know and control the software running on their own devices.

4.3 Encryption powers the security we need as a society for credit cards and commerce, patient data and medical information, proprietary business and legal discussions, and other important communications. As several leading cybersecurity experts articulated in a recent technical report, proposals to require a government backdoor into digital communications "are unworkable in practice, raise enormous legal and ethical questions, and would undo progress on security."[989]

5. Use of "equipment interference" impacting our company and our users

5.1 Similarly, compelling companies to modify their products to allow government access would deny UK businesses the ability to provide secure products and services to their customers, undermining trust and the success of UK businesses in the software and online service industries. For Mozilla, user trust is paramount, and any obligations introduced which would require us to undermine the security of the products and services we build and distribute would pose a significant challenge to our operations in the UK.

5.2 In particular, we are concerned about the expansion of unsolicited "equipment interference," or effectively intrusion, capabilities proposed in the Bill including:

- systems intrusion capabilities for law enforcement and intelligence agencies providing the ability to gain direct access to, or otherwise tamper with, electronic devices to obtain communications, private information or equipment data;[990]
- bulk intrusion capabilities for intelligence agencies for acquiring the content of communications;[991]
- extra-territorial reach of intrusion capabilities to "conduct" and "persons" outside of the United Kingdom;[992] and
- an obligation on Communication Service Providers (CSPs) to assist in giving effect to intrusion requests. These obligations would be imposed by the Secretary of

[989] http://dspace.mit.edu/handle/1721.1/97690
[990] Part 5, Equipment interference, Investigatory Powers Bill
[991] Part 2, Chapter 3, Investigatory Powers Bill
[992] Section 69, Extra-territorial application of Part 3, Investigatory Powers Bill

State onto "relevant operators" or "relevant operators of a specified description,"[993] and would include, but would not be limited to:

- (a) obligations to provide facilities or services of a specified description;
- (b) obligations relating to apparatus owned or operated by a relevant operator;
- (c) obligations relating to the removal of electronic protection applied by a relevant operator to any communications or data;
- (d) obligations relating to the security of any postal or telecommunications services provided by a relevant operator; and
- (e) obligations relating to the handling or disclosure of any material or data.[994]

5.3 The bulk systems intrusion provisions in the Investigatory Powers bill could be used to compel a software developer, like Mozilla, to ship hostile software, essentially malware, to a user — or many users — without notice. As an open source project, this is problematic from both philosophical and practical perspectives.

5.4 All Mozilla products are open source[995] and free software.[996] Not only is our software available for download free of charge, but also any user has access to the source code, and may freely modify and redistribute it. This means that changes to our software are fundamentally public. Were we compelled to create a version of Firefox that was modified to permit surreptitious intrusion subject to a government order, the modifications could and would be discovered by the Mozilla community.

5.5 Furthermore, any user may use the source code we provide to "build" their own copy of the software, whether the source code is modified from that which is publicly available or not. "Building" the code results in a program which reflects the code which was compiled, and which can easily be redistributed over the Internet. There is no technically feasible way for Mozilla to modify the source code during a user's independent build process. Thus, an unmodified version of the product will always be available to those with a little technical skill, and to anyone with whom those users have contact.

6. Duty not to make unauthorised disclosures

6.1 In light of the above, we are concerned about requirements to maintain the secrecy of surveillance capabilities built in to products and about the criminal penalties associated with violating that secrecy.[997] As outlined in Section 5, such restrictions on disclosure would not only contravene Mozilla's policies on notice and transparency, but would in many cases be technically infeasible as our products are open source and free software.

6.2 We believe that the wide use of open source software brings many benefits to users, businesses, and governments, and should be encouraged. The bill would instead create an

[993] Section 189, Maintenance of technical capability, Chapter 1, Part 9, Investigatory Powers Bill
[994] Section 184(4), Maintenance of technical capability, Chapter 1, Part 9, Investigatory Powers Bill
[995] http://www.opensource.org/docs/osd
[996] http://www.gnu.org/philosophy/free-sw.html
[997] Section 43, Duty not to make unauthorised disclosures, and Section 44, Offence of making unauthorised disclosures, Chapter 3, Part 2, Investigatory Powers Bill

environment of legal and practical uncertainty for Mozilla and other open source software developers and users.

7. Bulk interception compromising privacy of communications through passive surveillance

7.1 We are also concerned about bulk interception of communications data proposed in the bill. In particular:

- The interception of overseas-related communications;[998]
- The obtaining of related communications data from such communications, which can include data in transit or in storage;[999] and
- The obtaining of communications metadata[1000] and the content of communications.[1001]

7.2 We recognise that GCHQ and other country intelligence agencies currently engage in bulk collection of Internet communications. These practices fundamentally undermine the expectations of users of the privacy of communications and transactions online, and their lawfulness under European law is currently being considered by the European Court of Human Rights. We are concerned that this bill would explicitly legalise these harmful practices, when it should instead rein them in.[1002]

7.3 Security and privacy are essential parts of the user experience. We and other browser makers are pushing for a fully encrypted Web in order to protect users everywhere. The use of encryption is growing daily, protecting more and more communications from interference and interception. While some Web traffic remains unencrypted, the overwhelming majority of online traffic belongs to law-abiding citizens, and has no connection to any legitimate governmental purposes. We believe that all Internet users have an expectation of privacy in the network exchange of their communications, and companies and technologists continue to support this expectation through policy and through technology. Governments should not violate it to conduct bulk surveillance of innocent people.

8. Mandatory data retention

8.1 Finally, we have serious concerns with the mandatory data retention provisions, which would require CSPs to hold on to data for 12 months.[1003] As the Court of Justice of the European Union ruled in 2014, indiscriminate collection and storage of communications data is a disproportionate interference with the right to privacy.[1004] Mandatory data retention creates risk and undermines trust for the users of Firefox and other Mozilla products and services. Making troves of private user information vulnerable to malicious actors and holding user data longer than necessary for business purposes creates additional, and

[998] Section 106 (3), Bulk interception warrants, Investigatory Powers Bill
[999] Section 106 (7), Bulk interception warrants, Investigatory Powers Bill
[1000] Section 193 (5), Telecommunications definitions, Investigatory Powers Bill
[1001] Section 193 (6), Telecommunications definitions, Investigatory Powers Bill
[1002] Human Rights Organisations v UK, see: https://www.privacyinternational.org/node/555
[1003] Section 71, Powers to require retention of certain data, Part 4, Investigatory Powers Bill
[1004] Digital Rights Ireland v Ireland, see: http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=12322

unnecessary, liability and risk. As the nearly daily parade of data breaches make clear, amassing the personal information of everyone exposes those data to breach, theft, misuse, and abuse. Data acquired are data at risk, and such threat to user security and privacy is not warranted.

9. Conclusion

9.1 Thank you for the opportunity to comment on the draft Investigatory Powers Bill. As a global community of developers and engineers, Mozilla prides itself on providing secure and open products and services to our users. Mozilla sees the draft Investigatory Powers bill as a missed opportunity to set a strong global standard in reforming surveillance powers, and a harmful step backward for the interests of Internet users and the Internet economy. However, the UK parliament still has the opportunity to amend the bill, and we hope the Joint Committee on the Investigatory Powers Bill will carefully weigh the intended objectives with the consequences for the continued success of UK businesses and the security of users. Comprehensive revision of the draft Investigatory Powers bill is necessary to protect online commerce, and user privacy, security, and trust.

9.2 We look forward to working with you and the UK parliament to create meaningful surveillance reform over the next year, and are happy to answer any questions you may have.

21 December 2015

Cian C. Murphy and Natasha Simonsen—written evidence (IPB0096)

Introduction

1. This submission is made by Cian C. Murphy and Natasha Simonsen. We are both faculty members at The Dickson Poon School of Law, King's College London.

2. We welcome the effort to clarify and consolidate the law in the draft Investigatory Powers Bill. The existing legal framework has serious flaws. This process is an important opportunity to rectify those flaws and to construct a sound and enduring framework.

3. Our submission addresses three thematic areas, making a number of key recommendations in relation to each. The thematic areas are:

   A. The institutional infrastructure of the Office of the Investigatory Powers Commissioner;
   B. The process for authorisation of interception warrants by Judicial Commissioners;
   C. The need for fuller reform of the procedures of the Investigatory Powers Tribunal.

4. Prior to addressing these issues, we set out here a preliminary concern. This concern relates to the absence of clear definitions of key terms in the draft Bill. In particular, the term 'internet connection records' is not a term which is defined in existing law or which, to our knowledge, is in common use (whether in technological operations or otherwise). The absence of a definition of this important term is significant because the mechanism by which state authorities may access different types of data varies depending on the type of data in question. It is imperative that the definition of this key term be made clear if there is to be meaningful scrutiny of the powers set out in the draft Bill, both in Parliament and in public debate.

A. Institutional Infrastructure for Oversight

5. We support the proposal to establish an Office of the Investigatory Powers Commissioner. We consider this proposal to have the potential to significantly improve the existing system of three separate commissions with different areas of responsibility and oversight. However, we make two recommendations about the nature and structure of the Commissioner's Office.

   1. **First,** it is crucial that there be a clear separation between the work of those Judicial Commissioners responsible for the authorisation of warrants, and the work of those individuals within the Office who bear responsibility for oversight and auditing. It is vital for the maintenance of public trust in the institution that the latter functions be clearly insulated from the former.

   2. **Second,** we recommend that the Judicial Commissioners be appointed by the Judicial Appointments Commission. The draft Bill places upon the Judicial

Commissioners an obligation to serve in what is, in effect, a quasi-judicial role. We recommend (below) that that role be made as close to a judicial role as possible - a key part of which is appointment through an appropriate process. We consider that appointment through the Judicial Appointments Commission will build public confidence, and is more likely to command the respect of overseas stakeholders, including foreign Governments and communications service providers.

B. Authorisation of Interception Warrants

6. We welcome the proposal in the draft Bill to require the involvement of 'Judicial Commissioners' in the authorisation of interception warrants. This represents an improvement on the existing process for executive approval, which is both impractical (given the volume of interception warrant requests), and lacks safeguards. However, we recommend four changes to the processes set out in the draft Bill.

1. **First,** the language in the draft Bill should be amended to require that warrants be 'issued' rather than 'approved' by a Judicial Commissioner. This shift in language would be subtle but significant. The language in the draft Bill states that the Secretary of State 'may … issue' a warrant (section 14(1)). This issuance is then 'approved' by a Judicial Commissioner. This approach strikes the wrong balance between executive and judicial (or quasi-judicial) powers. We note that a different method of decision-making may be followed by Judicial Commissioners who must merely 'approve', rather than 'issue' warrants. Whereas the latter requires a *de novo* decision to be made, the former merely reviews an existing decision (of the Secretary of State). We further note that the instruction in the draft Bill to apply 'the same principles as … on an application for judicial review' (section 19(2)) might be understood to further reduce the level of scrutiny by Judicial Commissioner – in particular if the national security context were used to dictate a 'light touch' rather than an 'anxious scrutiny' review. To avoid these problems arising, and there being merely the appearance of independent review, we therefore recommend that those sections that relate to the issuance of warrants be amended. The sections, as amended, should state that an intercepting authority may 'apply' for a warrant subject to the 'consent' of the Secretary of State, with the decision to 'issue' the warrant falling to the Judicial Commissioner.

2. **Second,** we consider that a case has not yet been made for the need for an 'urgent' procedure to bypass the need for prior approval (or, as we would have it, issuance) by a Judicial Commissioner *before an interception operation commences*. We accept that there may be circumstances where a warrant is needed on short notice. However, the ordinary process envisaged by the draft Bill is plainly designed to be swift. The ordinary process, for instance, is *ex parte* rather than adversarial. The Government therefore needs to make a more compelling case for the 'urgent' procedure or to remove this aspect from the Bill.

3. **Third,** if the need for 'urgent warrants' is established, the legislation should specify the grounds necessary to trigger the urgent process. At present, the draft Bill merely requires that 'the person who issued the warrant considered that there was an urgent need to issue it' (section 20(1)(b)). This language sets a low bar for the issuance of such a warrant. We are conscious of the need to ensure there is sufficient discretion for those who take such decisions to do so on the basis of operational necessity. However, we consider that the inclusion of a *non-exhaustive list of examples* in which issuance is appropriate would provide Judicial Commissioners with an indication of the *types of circumstance* in which it would be appropriate to issue such a warrant without putting too great a limit on the operation of the system in practice.

4. **Fourth**, we draw the Committee's attention to the need for procedures for retention and disclosure of information relating to applications and warrants. For instance, there may be circumstances in which disclosure to the subject of a warrant is appropriate. These circumstances could include: (i) where an unsuccessful application for a warrant has been made; (ii) where a warrant has expired, and its existence is no longer operationally sensitive; (iii) where an application is made under the Freedom of Information Act 2000, and/or; (iv) where disclosure is ordered in subsequent legal proceedings. Consideration should be given to addressing these matters either in the Bill or in the accompanying regulations.

7. We consider that these recommendations would facilitate more effective scrutiny of interception warrants and thereby improve the operation of the system. We also believe that this effectiveness, and greater scrutiny, need not come at the cost of efficiency. Judicial Commissioners may develop expertise in the authorisation of warrants that would leave them as competent, and over time more competent, than a Secretary of State - not least as the terms of Secretaries of State are much more variable than those of Judicial Commissioners need be.

8. As a further consideration, we believe that these improvements would also send a strong signal to the British public, and to international stakeholders with which Britain may seek to co-operate on investigatory powers, that there is a robust system of authorisation in place for interception warrants.

C. Reform of the Investigatory Powers Tribunal

9. We welcome the draft Bill's introduction of a right of appeal from the Investigatory Powers Tribunal to the Court of Appeal (in England and Wales). It implements a common recommendation of the Intelligence and Security Committee, Anderson, and Royal United Services Institute reports. However, we also consider that the operation of the Investigatory Powers Tribunal could be improved in five key ways by amendments to the draft Bill.

1. **First,** we recommend that the Tribunal be given a power to order disclosure. The power of a court or tribunal to make orders that bind the parties is a

cornerstone of the rule of law. The absence of such a power for the present IPT is anomalous and unsatisfactory.

2. **Second**, we recommend that the draft Bill specify that judges on the Investigatory Powers Tribunal be appointed by the Judicial Appointments Commission. The current appointment process is a further anomaly in the context of the wider justice system and may undermine public confidence in the institution.

3. **Third,** we believe that the use of special advocates before the Tribunal merits further consideration. We are conscious of the conclusion in the Anderson Report that counsel to the Tribunal may be more effective than special advocates (para 14.108). However, the adversarial principle is central to the effective operation of British justice and, in the absence of an advocate on behalf of the applicant in closed proceedings, we have concerns about whether this principle can be properly respected. We note that others, in particular JUSTICE, have made strong arguments in favour of the use of special advocates before the IPT, and we consider that this question merits sustained debate during the legislative process.

4. **Fourth,** we note the proposal in the Anderson Report, that the Tribunal have the power to hear complaints against communications service providers, has not been adopted in the draft Bill. Given the significant role that communications service providers have in interception and data retention, judicial scrutiny of their operations is salient to both the effective working of the system and to public trust in the system.

5. **Fifth,** as a final point, we agree with the RUSI report that the Tribunal should work to improve the openness of its operation and become less opaque. In general we consider that the Tribunal should take the Administrative Division of the High Court as its benchmark for open and transparent procedures, and should deviate from that benchmark only insofar as is absolutely necessary, in light of the nature of the Tribunal's work.

Conclusion

10. Overall we welcome the Government's efforts to take the best of the three reports on investigatory powers and produce a comprehensive new law. We consider that the draft Bill is a useful first step in the legislative process. However, we also consider that there remains much scope for improvement in the Bill in the course of the legislative process. The above recommendations represent some, but by no means all, of the ways in which such improvement could be brought about.

Cian C. Murphy & Natasha Simonsen
21 December 2015

Muslim Council of Britain—written evidence (IPB0095)

About us:

The Muslim Council of Britain is the UK's largest Muslim umbrella body with over 500 affiliated national, regional and local organisations, including mosques, charities and schools. The overriding objective of the Muslim Council of Britain is to work for the common good.

1. Introduction

1.1. The Draft Investigatory Powers Bill (the **Bill**) presented to the two Houses in November 2015, is aimed at providing the police and intelligence services with a broader and more modernised set of tools to keep our nation safe.

1.2. The Muslim Council of Britain (**MCB**) strongly supports the government's and law enforcement agencies' objective of ensuring the safety of the public and preventing terrorism.

1.3. In today's society where terrorists, paedophiles and other serious criminals have the ability to use more sophisticated technology, there is no doubt that a modernisation of the capabilities of our police and intelligence services is important to consider.

1.4. Any changes to the legal scope of powers must be necessary and proportionate, with an appropriate balance between security, civil liberties and the impact on communities.

2. Civil Liberties

2.1. Many of our affiliates have raised concerns about the Bill's impact on civil liberties and whether there are sufficient safeguards enshrined in the proposal to protect our civil liberties.

2.2. There is a particular concern about whether the judicial authorisation for interception warrants within the Bill is sufficiently robust to provide reassurance to the public that such serious action was necessary and proportionate.

2.3. An in-depth analysis of this and the broader concerns surrounding civil liberties will remain outside the scope of this submission and are being addressed separately in submissions from civil liberty groups and experts.

3. Impact on Communities

3.1. There are many examples of legislation enacted in the past whose implementation has been unfairly discriminatory or disproportionate, or at least perceived to have been discriminatory and disproportionate, with a subsequent impact on communities.

3.1.1. **Stop-and-Search:** It has been acknowledged by the Home Secretary that rather than being intelligence-led, stop-and-search powers have been misapplied, leading to them being seen as sharply divisive in Britain's black and minority ethnic communities. She argued that their implementation needed to evolve to ensure their fair and effective use.[1005]

3.1.2. **Counter-Terrorism and Security Act (CTS Act):** During the passage of the CTS Act, the MCB highlighted the perception of Muslim communities that previous legislation has been used in a discriminatory fashion against Muslims in particular.[1006]

The MCB requested that there be adequate safeguards, sufficient provisions for judicial oversight and the appropriate levels of transparency in place to reassure the public that there would be no discrimination in the implementation of these expanded powers.

The concern was that unless the Bill goes to great lengths to demonstrate that it is 'blind' to cultures or religious beliefs, it risked further losing the goodwill and support of the Muslim community, who are wary of being singled out.

Case studies collated by the MCB and included by David Anderson QC as part of his annual report demonstrate the foreseeable discriminatory application of the CTS Act.[1007]

3.2. To learn the lessons from previous legislation, the MCB has two recommendations to reduce the risk of discrimination in the implementation of this Bill (if/when it comes into force) and the subsequent impact on communities:

3.2.1. **Recommendation 1:** The mandate of the Investigatory Powers Commissioner (IPC) should explicitly include a specific duty to monitor, track and report on discrimination in the implementation of the law. Any identified pattern of discrimination should be appropriately explained, with steps articulated as to how this can be resolved.

3.2.2. **Recommendation 2:** There should be safeguards included within the guidelines provided to practitioners of the law that explicitly explain that Muslims and those of any faith or ethnic group, should not be treated differently to those of others or no faith.

21 December 2015

[1005] Hansard for Wednesday 30 April 2014: http://www.publications.parliament.uk/pa/cm201314/cmhansrd/cm140430/debtext/140430-0001.htm#14043038000267

[1006] http://www.mcb.org.uk/wp-content/uploads/2015/01/MCB-Briefing-on-safeguardsrequired-to-prevent-discriminatory-application-of-the-Bill.pdf

[1007] http://www.mcb.org.uk/wp-content/uploads/2015/10/20150803-Case-studies-about-Prevent.pdf; also available in Annex 2 of https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/09/Terrorism-Acts-Report-2015-Print-version.pdf

National Union of Journalists (NUJ)—written evidence (IPB0078)

1. The National Union of Journalists (NUJ) is the representative voice for journalists and media workers across the UK and Ireland. The union was founded in 1907 and has 30,000 members. We represent staff, casuals and freelances working at home and abroad in the broadcast media, newspapers, news agencies, magazines, books, public relations, communications, online media and photography.

2. The NUJ welcomes the opportunity to provide evidence to the joint committee in response to the draft Investigatory Powers Bill (IPB).

3. The history of the police and intelligence agencies in the UK over the last 50 years has included the monitoring, infiltration and targeting of journalists, trade unionists and social justice campaigners. For example, in November 2014, six NUJ members launched a collective legal challenge in response to finding themselves listed on a secret police database of "domestic extremists". The database includes intimate details about their lives, including their work, their medical history and even their sexuality. Their lawful journalistic and union activities have been monitored and recorded.

4. It is in this context that there is a compelling case for proper parliamentary scrutiny and debate about the draft IPB and there is a need for much stronger oversight of surveillance powers by both parliamentarians and the judiciary.

5. It is the state’s concerns that dominate the draft IPB whilst the associated human rights, civil liberties, privacy and related concerns of UK citizens are mostly absent from the proposed legislation. However, this submission is largely focused on the impact of the IPB on journalists and journalism.

6. In the UK, journalists have been spied on, their phone records secretly pored over and their communications seized. This has significant implications for NUJ members and for upholding the union's longstanding ethical code of conduct. The NUJ's code has established the main principles of UK and Irish journalism since 1936. The code is part of the union rules; members support the code and strive to adhere to its professional principles. The NUJ code of conduct includes the following clause:

7. "A journalist protects the identity of sources who supply information in confidence and material gathered in the course of her/his work."

8. Michelle Stanistreet, NUJ general secretary, said: "We are defending the core principle enshrined in the NUJ's code of conduct - the protection of sources. It is a vital aspect of a free press - that whistleblowers and sources need to be able to come forward and share information they believe the public should know about in the certain knowledge that their identifies will be protected.

9. "We are raising awareness of the growing threat to the ability of journalists to do their jobs safely, to guarantee their material and to protect their sources. Without that protection, we simply won't have a functioning free press.

10. "We cannot have a situation where journalists are seen as instruments of the state - their work should not be used by the authorities as a short cut in their investigations, and their sources shouldn't in any way be compromised or identified."

11. In relation to the NUJ's code of conduct, we believe the current proposals contained within the draft IPB do not allow journalists to protect the identity of sources or provide sufficient protections for journalists' materials and communications.

12. The right to protect journalistic sources is recognised by international law. It has been recognised by the United Nations, the Council of Europe, the Organisation of American States and the Organisation for Security and Cooperation in Europe. The European Court of Human Rights said in several of its decisions that it's a key element of freedom of expression. In addition, the NUJ has historically secured legal precedent on the protection of sources in the Goodwin v UK 1996 case. The Goodwin judgement stated:

13. "Protection of journalistic sources is one of the basic conditions for press freedom"

14. In order to be able to play the role of watchdogs, as qualified by the European Court of Human Rights, journalists need to rely on sources of information. Some of these sources are official and known, but more often, they're confidential and secret. Without protection, some informers will refuse to speak out, for fear of being exposed.

15. One of the most serious consequences of the lack of protection is the impact on the physical integrity of journalists. This applies to journalists who work in dangerous environments such as war zones and/or those who investigate organised crime. If journalists are perceived as informers to the authorities, or as future witnesses in a trial, they can become a target. Furthermore, a lack of safeguards for all journalists will have profound consequences for the public's right to know. As Chris Frost, the chair of the NUJ ethics council, has said: "It is difficult to measure the extent of stories from whistleblowers because they are anonymous but in my experience virtually every serious investigation is launched on the back of a source or whistleblower who needs to be kept anonymous for their protection."

16. It is the NUJ's view that the draft IPB should include stronger measures to safeguard journalists and their sources. There is no fundamental difference between the authorities asking for a journalists' physical contacts book or footage and their telephone and communications records. The effect on journalists and sources is exactly the same and the same legal safeguards must cover both.

17. Source protection does not just apply to the identity of the source but also to all matters relating to and communications between the journalist and the source. This

includes the person's name; personal data, voice and image. It also includes the unpublished content of information and the circumstances of acquiring the information.

18. The NUJ is calling for specific changes to the IPB to include:
    - Automatic and mandatory prior notification
    - An independent and judicial process
    - Mechanisms to challenge an application with the right of appeal

19. Under the Police and Criminal Evidence Act (PACE) journalists are notified when the authorities want to access their material and sources, and journalists have the ability to defend their sources in an open court with the chance to challenge and appeal the application and related decisions. Unlike PACE, both RIPA and the draft IPB do not apply the same protections and safeguards.

20. In the draft IPB it states that "in making an application for data to identify a journalistic source, the applicant is not required to notify either the person to whom the applications relates i.e. the journalistic source, nor that person's legal representative".

21. Without prior notification a journalist and/or media organisation will not have an opportunity to challenge this behind-the-scenes request. This means that the public interest and press freedom arguments for maintaining source protection are never put forward.

22. The NUJ has routinely tackled and challenged cases where the police have served production orders on journalists - we've funded and supported journalists through lengthy and stressful legal processes in which they have successfully stood up for their sources, and stood by the NUJ's code of conduct. But if journalists don't know their data is being snooped on and their sources spied on, how can a journalist defend themselves and the long-held principles they stand for?

23. Dominic Ponsford, editor of Press Gazette, has also emphasises the risks involved: "If law enforcement are able to secretly grab the phone records of journalists and news organisations then no confidential source is safe and pretty much all investigative journalism is in peril."

24. In the case of Tom Newton Dunn, the police used RIPA to access his phone records in secret. They did not notify him that they had accessed his material or sources. The police obtained the phone records without notification or consent and in other RIPA cases, when the police have been spying on journalists no journalist was informed in advance.

25. Roy Mincoff, NUJ legal and industrial officer, said: "To continue to allow the authorities to access journalists' data and therefore sources will have a serious chilling effect on those who would otherwise reveal corruption, crime, abuse and

wrongdoing by public and private bodies. Journalists are the public watchdog, with a duty to inform the public. The public has a right to be informed."

26. In November 2015 and when asked about protection of journalistic sources in parliament, the home secretary Theresa May said: "We will put into this legislation what we put into PACE code earlier this year, which is that for access to communications data to identify a journalist's source, it will require judicial authorisation."

27. Clause 61 of the draft IPB refers to the approval of a "judicial commissioner" before accessing journalists' communications data yet there is no provision for a journalist or media organisation to be able to contest an application before a judge (or appeal) in advance of the investigatory power being granted. The draft IPB appears to propose to review a decision that has already been taken and merely check if the correct procedure has been followed. This is not the same as a judge hearing the arguments for and against.

28. In the draft IPB this oversight will only apply for the purpose of an application that attempts to identify a journalistic source and the judicial authorisation set out in the draft IPB will only cover the police and not the intelligence services. There is no prior right of notification for journalists or media organisations where their material is either deliberately, incidentally, collaterally or accidentally sought or obtained, whether by the police or by intelligence agencies and the proposed measures can be bypassed by using the urgency procedures.

29. The NUJ believes the production order procedures set out in PACE - in which a judge makes the decision and has the benefit of evidence and argument from the journalist as well as the state - offers better safeguards and protections than what is proposed in the draft IPB. This is because PACE includes the right to challenge and appeal. Unlike PACE, the draft IPB contains no reference to a right of source protection that can only be displaced by an overriding public interest. There are also no measures proposed in the draft IPB that would compel the police to exhaust other lines of inquiry in the first instance and in advance of an application that attempts to identify a journalistic source.

30. Gavin Millar QC has said: "There must be an overriding requirement in the public interest - in order to remove the source protection. This is a very high hurdle and is not specified in the bill… Under the bill the journalists' data can be obtained in any criminal investigation, however minor.

31. "The intelligence services are excluded from the requirement to obtain even this (flawed) form of judicial approval. Yet the convention law applies to them just as much as to the police who obtain source-identifying information.

32. "Both under the Police and Criminal Evidence Act 1984 and the Terrorism Act 2000 when the police apply for orders for material in the possession of the journalist to be

handed over (known as production orders) there must be a hearing before a judge at which the journalist is entitled to be heard.

33. "The worry is that the police will now start using these powers routinely to identify sources instead of making PACE/TA applications for the journalist's material."

34. The draft IPB provides an easier route for the authorities to identify a journalists' source when it is compared to the tried and tested legislative framework that already exists under PACE. The NUJ is also concerned by the powers on "equipment interference" that enable the authorities to access computers or other devises. This means the authorities would have control over targeted devices and access to any information stored. This information could include documents, emails, diaries, contacts, photographs, internet messaging chat logs, and the location records on mobile equipment. It would also mean having powers to access anything typed into a device, including login details/passwords, internet browsing histories, other materials and communications. Draft documents and deleted files could also be accessed. In addition, the microphone, webcam and GPS-based locator technology could be turned on and items stored could be altered or deleted. These powers accompanied by the proposals to retain 12 months' of website data of all UK citizens have severe and detrimental implications for investigative journalism.

35. In conclusion, the draft IPB needs better safeguards across the entire draft bill - not just in the section relating to the interception of communications data. For example, the protections specified for journalists should also apply to related powers of collection, retention and examination. The revelations that the police had been routinely using - or rather misusing - the RIPA codes to secretly access information on journalists and their sources sent genuine shock waves throughout our industry. It has also united organisations and individuals that often do not rub shoulders together - just within journalism. We are now starting to see the same alliance speak out to raise genuine concerns about the lack of safeguards proposed in the draft IPB so we hope the joint committee will be persuaded by our specific concerns and the alternative proposals suggested.

21 December 2015

Professor John Naughton and Professor David Vincent—written evidence (IPB0131)

1 John Naughton is a Senior Research Fellow in the Centre for Research in the Arts, Social Sciences and Humanities (CRASSH) in the University of Cambridge, an Emeritus Fellow of Wolfson College, Cambridge and Emeritus Professor of the Public Understanding of Technology at the Open University. He is the author of two books on the history and implications of the Internet and is the Technology columnist of the *Observer* newspaper.

2 David Vincent is Emeritus Professor of Social History and a former Deputy Vice Chancellor of Keele University and the Open University. He is a Visiting Research Fellow in the 'Technology and Democracy Project' at CRASSH in the University of Cambridge and the author of books on the history of privacy and public secrecy.

3 An important question that the Joint Committee wishes to consider is whether the case been made, both for the new powers authorized in the proposed legislation and for the restated and clarified existing powers.

4 A persuasive case has been made for the clarification of some existing powers. The inadequacies of RIPA highlighted by David Anderson QC have been addressed and the wording in the draft bill represents a significant improvement on what went before. Likewise, it is an advance to have the bulk surveillance powers granted by the Telecommunications Act 1984[1008] explicitly described for the first time.

5 However the general case made for the new powers is unsatisfactory in a number of ways. It suffers from the same flaws as earlier justifications, namely that it is based purely on official assertions that the powers are necessary, together with implicit assertions that they are effective in achieving stated aims.

6 This may well be the case, but since no publicly-available evidence in support of these assertions is provided, the public has no way of assessing the strength of the case that is being made, or indeed of challenging it. So essentially the official argument for the powers sought can be reduced to a simple proposition: "Trust us; we need these powers".

7 In this context it is significant that the tone of public justifications offered by ministers for this draft legislation has been mostly assertive and emotive. The grounds for surveillance are more tightly drawn in the draft bill than previously, but the popular conception, promoted by government -- that we are mainly concerned with ISIS and paedophiles -- is not borne out by the text of the draft Bill.

8 For example, the flow chart on p18, explaining the process for Equipment Interception Authorisation for MI5, SIS, GCHQ, and Armed Forces has as its first box: 'Is the warrant for national security, serious crime or EWB [Economic Wellbeing]?' (s 169 (5 b i-iii)) This trinity is derived from Article 8 (ii) of the European Convention on Human Rights (ECHR) which specifies that the right to privacy in Article 8 (i) can be overridden "as is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of

[1008] https://www.opendemocracy.net/digitaliberties/julian-huppert/1984-revisited

the country", and is presumably intended to protect the proposed interception regime from action under the 1998 Human Rights Act.

9 Whatever "economic wellbeing" meant to the drafters of the ECHR, its definition now is far from clear. At face it appears to be an ideologically-charged defence of a particular set of economic arrangements. It is glossed in the Bill as 'the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security" (s 13 (3 c)), which renders the issue redundant - if it only relates to national security it can be subsumed within that category - yet the phrase continues to be used without further explication throughout the Bill. While it may be reasonable to accept intrusive surveillance for the purposes of ensuring the safety of all citizens, it is questionable to deploy the same measures merely to ensure the prosperity of some citizens rather than others. It would therefore seem appropriate that the purpose of "economic well-being" should receive critical scrutiny by Parliament.

10 The ostensible function of the Investigatory Powers Bill is further diluted by Part 3 of the Draft, which covers the significant power to obtain communications data. In her Foreword to the consultation paper, the Home Secretary writes, "Powers to intercept communications, *acquire communications data* and interfere with equipment are essential to tackle child sexual exploitation, to dismantle serious crime cartels, take drugs and guns off our streets and prevent terrorist attacks." (emphasis added) However the grounds for obtaining communications data set out in the Draft Bill (s 46 (7 a-j)) are much more widely drawn. Whilst a targeted interception warrant is for the "purpose of preventing or detecting serious crime", the qualifier "serious" is omitted when it comes to obtaining communications data. Now the criterion is simply "preventing or detecting crime or of preventing disorder". Any level of potentially criminal or disorderly conduct will justify an invasion of private communication. The breadth of these powers is further illustrated by the table of "Relevant Public Authorities and Designated Senior Officers" in Schedule 4 (pp. 210-14) which include not only the police forces and security services, but fraud officers in the Department for Work and Pensions, and the "Deputy Chief Inspector in Trading Standards Services".

11 The draft Bill rests on two claims, that it clarifies the nature of investigatory powers and that it provides effective oversight of their exercise by independent judicial commissioners. But if the Bill fails on the first claim because of the vague and open-ended grounds for surveillance, it fails on the second. The boundaries between what is legitimate and illegitimate warranted interception and what is acceptable and unacceptable data retention, will remain impossible to draw with sufficient clarity to engender public confidence in the entire process.

12 The absence of publicly available evidence of the effectiveness of bulk collection capabilities in achieving their stated aims is a pervasive problem facing democratic societies. In 2013, for example, President Obama's Review Group on Intelligence and Communications Technologies examined 225 terrorism cases from 2001 onwards and concluded that the NSA's bulk collection of telephone records was "not essential to preventing attacks".[1009] On the other hand, one member of the Presidential Panel, Michael Morrell (who agreed with the above

[1009] Ellen Nakashima, "NSA phone record collection does little to prevent terrorist attacks, group says", *Washington Post*, January 12, 2014.

conclusion) nevertheless observed that "Had the program been in place more than a decade ago, it would likely have prevented 9/11. And it has the potential to prevent the next 9/11. It needs to be successful only once to be invaluable."[1010]

13 What this highlights is the difficulty – or perhaps the impossibility – of having an informed public debate about the extent and pervasiveness of surveillance that is justifiable. Online surveillance may well be as effective at forestalling terrorist attacks as ministers maintain. But some terrorists will always get through – as for example in Paris in November 2015. And the resulting outrage will spur popular, media and political demands for yet more surveillance powers. So we are likely regularly to be faced with the question: *how much surveillance is enough?*

14 This may be inevitable in the case of 'national security' which lies, almost by definition, outside the realm of cost-benefit analysis. But national security is not the only purpose listed in the draft Bill.

15 Much of the official rhetoric about the need for the new powers seeks to frame the issue in terms of 'striking a balance' between privacy and security. Unlike David Anderson's recent report, *A Question of Trust*, no attempt is made to assess the nature and value of privacy, or to examine the trade-off between privacy and security in a modern democratic society. The draft Bill is disingenuous because it implies that privacy is a private good whereas security is a collective one. But privacy is both a private *and* a collective good. A society in which surveillance becomes so intrusive that citizens never know if they are being watched is not a healthy one, because everyone has a right to, and a need for, a truly private life. Citizens of a democracy are entitled to both privacy *and* security.

16 There is a further concern that the draft Bill deals inadequately with conflicts with existing protections of privacy. In respect of confidential information held by "one of the sensitive professions", actions are to be policed by "Codes of Practice" which are not legally binding. (p. 28) All that is required is that the law enforcement and security agencies must make a "compelling case" to obtain, for instance, legally privileged information. This reduces the protection of privacy to a private dialogue between the Secretary of State and the interceptors.

17 Another question that the Committee will wish to consider is whether the technological definitions (e.g. of 'content' vs. 'communications data', and 'internet connection records') in the draft Bill are accurate and meaningful. In our opinion, definitions of the various kinds of information and communications covered by the draft are unsatisfactory.

18 In the explanatory notes that precede the text of the Bill it is claimed (p.5) that the legislation "will make sure powers are fit for the digital age. The draft Bill will make provision for the retention of internet connection records (ICRs) in order for law enforcement to identify the communications service to which a device has connected. This will restore capabilities that have been lost as a result of changes in the way people communicate."

19 This attempt to future-proof the proposals is undermined by the uncertainty about whether, at what cost and at what speed, the Communication Service Providers (CSPs) can manipulate the current systems in the interests of greater

[1010] Michael Morell, "Correcting the record on the NSA recommendations", *Washington Post*, December 27, 2013.

surveillance, let alone any future communication technology. It is not clear that it is technically feasible to retain and store bulk ICRs within a foreseeable timeframe and budget.

20 Since the Snowden revelations, the CSPs have been increasing the encryption of data they transmit in response to user concerns, and there is a very real danger that the requirement to "remove any encryption applied by the CSP to whom the notice relates" (p. 29) will either be technically difficult, or, if successful, will weaken the security of individual users, and of the material held by the CSPs. Although the Bill provides a new offence of "knowingly or recklessly" obtaining "communications data from a telecommunications operator or postal operator without lawful authority" (s 8(1)), the task of protecting such data will be made more difficult by the de-encryption requirement.

21 Clause 71 stipulates that Internet service providers will be required to keep ICRs for a maximum period of 12 months. In the Explanatory Notes, Internet connection records are defined as "a record of the internet services that a specific device connects to – such as a website or instant messaging application – captured by the company providing access to the internet. They could be used, for example, to demonstrate a certain device had accessed an online communications service but they would not be able to be used to identify what the individual did on that service."

22 Given the centrality of the requirement to retain ICRs it would be reasonable to expect a clear technical definition of what an ICR is within the meaning of the proposed legislation. But none is given.

23 What is even more striking is that leading technical experts in the industry are puzzled by what an ICR consists of and what collecting such records would involve. According to the relevant industry body, the Internet Services Providers Association, for example, "ICRs are not currently retained or held by service providers for business purposes, i.e. they are an artificial construct that, depending on how the definitions of the Bill are interpreted, will require services providers to produce large volumes of new data sets."[1011] Evidence from BT says that "Leaving aside issues relating to the definitions of ICR contained in the Bill (there are two), BT does not currently generate (or retain) a single set of data that is capable of meeting the proposed requirement."[1012]

24 In that context, Ministerial resort to analogue metaphors in an attempt to explain this legislation to Parliament and the public is unfortunate. In her Statement to the House of Commons on November 4, for example, the Secretary of State said that an Internet Connection Record was "simply the modern equivalent of an itemised phone bill". This is a deeply misleading analogy, because – whatever it turns out to be – an ICR in the current technological context will be significantly more complex and harder to compile than an itemised bill. The danger is that MPs will have been given the impression that the requirement on

[1011] Internet Services Providers' Association, evidence to Select Committee on Science and Technology, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25540.html

[1012] British Telecom, Evidence to Select Committee on Science and Technology, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25410.html

Communications Services Providers to collect and retain ICRs is a relatively straightforward matter. This is unlikely to be the case.

25 The draft Bill's vagueness about ICRs may reflect official uncertainty about the complexity and variety of the ways in which users and devices currently interact with communications services – in other words an understandable reluctance to freeze in statute a concept that is constantly evolving. But without a technologically-literate and coherent definition of ICRs the Bill is unworkable as it stands. The absence of such a definition makes it difficult to assess what data could fall under the Act and what impact the collection of this data may have on businesses and consumers.

26 The dangers of 'freezing' in primary legislation detailed technical specifications relevant to a fast-evolving technology are widely conceded and understood. How then is Parliament to resolve the conflict between the need to be legally precise without having to re-legislate every two years?

27 The solution envisaged by the drafters of the Bill is to use "Codes of Practice" which can regularly be updated. This was the strategy employed, for example, with RIPA. If this is the approach adopted for the Investigatory Powers Bill, then two concerns must be addressed.

28 The first is – as Sir David Omand observed when giving evidence to the Select Committee on Science and Technology – the need "to learn from the mistake that the Home Office made over the last five years, which was not to update the codes of practice, so that we, the citizens, knew how the existing legislation was being used. They could have done that, in which case the Snowden case would not have been the shock, horror that apparently it was for many people. Those codes of practice are presented to Parliament. You can insist that they are revised. You could put that in your legislation. There are ways in which the Government at any one time can be quite precise about how it is interpreting them, which will help the judges very considerably. That can then be updated."[1013]

29 The second is that these Codes of Practice have to be legally binding, rather than purely advisory or informative.

30 In one respect, the draft Bill represents a 'tidying up' exercise – putting powers available under a patchwork of other laws into one over-arching statute. This is a welcome development. But viewed from this perspective, one entirely new power is being sought – that of 'Equipment Interference' (EI).

31 This is a euphemism for what in the computer science community would be called "authorised hacking". We know from various sources -- the Snowden revelations, for example, and expert testimony to the Investigatory Powers Tribunal[1014] -- that such covert activities, authorised by a number of other statutes, have for some time formed part of the technical armoury of GCHQ.

32 The term 'Equipment Interference' covers a wide variety of ways in which communications and computing equipment can be covertly penetrated, used for surveillance purposes, destroyed, rendered inert or otherwise subverted. A classic example (allegedly possible using commercially-available technology)

[1013] http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/oral/24378.pdf

[1014] In the cases brought by Privacy International and a number of CSPs against the Foreign Secretary and GCHQ.

enables an attacker covertly to activate the camera and microphone of a smartphone, thereby turning it into a remote monitoring device. Most if not all of the known EI techniques are illegal under domestic legislation like the Computer Misuse Act 1990.

33 Publication of the draft Bill represents the first explicit public admission that such activities are practised by the security and intelligence agencies, and sets out a regime under which they can be authorised and regulated in the future.

34 The agencies that will be licensed to use EI are law enforcement, the security and intelligence agencies, and the armed forces.

35 Two kinds of EI are identified in the draft Bill – 'targeted' and 'bulk'. Warrants for EI must be approved by a Judicial Commissioner and law enforcement agency warrants will only be issued for investigation of 'serious crime'.

36 We can see that there is a reasonable case for *targeted* EI, and are of the opinion that the proposed authorisation regime is robust.

37 However the proposal for *bulk* EI powers raises concerns on several grounds:

(a) Bulk warrants will be issued only to the security and intelligence agencies and must be focused on obtaining data relating to persons outside the UK; the proposed legislation therefore represents a significant extra-territorial expansion of state power;

(b) The fact that EI is regarded as lawful in the UK may undermine overseas confidence in British IT products and services, which would then be regarded with the suspicion that Chinese networking products are currently viewed in the US and UK;

(c) More importantly, it could, in some circumstances undermine confidence in the global Internet environment;

(d) Hacking is a creative activity and – like innovation in financial services – can be very hard to regulate and control.

But the most worrying concern is that as the 'Internet of Things' expands, and billions of devices become networked, bulk EI could have unintended consequences which might prove very counter-productive to the interests of the UK. We therefore recommend that the proposal for authorisation of bulk EI should be skeptically scrutinised by the Committee.

John Naughton
David Vincent
Technology and Democracy Project
Centre for Research in the Arts, Social Sciences and Humanities
University of Cambridge

21 December 2015

Network for Police Monitoring (Netpol)—written evidence (IPB0087)

1. The Network for Police Monitoring (Netpol) is a network of organisations with an interest in monitoring or observing policing. This includes those based within a set community, such as the Newham Monitoring Project, and those that work directly with protest, such as the Green and Black Cross, who train and support legal observers. Netpol acts as a focus for campaigns relating to aspects of policing that are viewed as excessive or oppressive.

2. This submission is concerned with the legality of the proposed Bill, and provides a response, in particular, to the following questions posed by the Joint Committee on the Draft Investigatory Powers Bill:

> Are the powers compatible with the Human Rights Act and the ECHR? Is the requirement that they be exercised only when necessary and proportionate fully addressed? Are they sufficiently clear and accessible on the face of the draft Bill?

3. This submission addresses the exercise of surveillance powers by law enforcement agencies. It does not address the role of the security services or the use of bulk interceptions of bulk datasets.

Are the powers compatible with the Human Rights Act and the ECHR?

4. Our concern is that the Bill enables highly intrusive surveillance practices in response to activities protected under articles 10 and 11 ECHR (rights to freedom of expression and assembly) and that the requirements of legality are not met. These requirements are such that that legislation must ensure that the scope of discretion to be exercised by the state is made clear, and that there is an adequate indication of the nature of the offences that may give rise to such intrusive activities[1015].

5. The Investigatory Powers Bill is not clear as to the circumstances in which intrusive surveillance may be carried out in relation to collective activity. While the Bill suggests that practices of interception and equipment interference may be carried out only for the purpose of addressing serious crime, the effect of the Bill will be that protest groups carrying out collective activities may be subject to such surveillance for much broader purposes, including the prevention and detection of minor offences.

6. The broad scope of the Bill in relation to the surveillance of collective activities and the meaning given to 'common purpose' means that it falls to considerations of proportionality and necessity to constrain state actions. Policing units, however, will retain a great deal of operational discretion. Without further guidance as to the circumstances in which the surveillance of protest groups will be both necessary and

[1015]This requirement has been frequently stated in the case law of the ECtHR. See, for example, Weber v Germany (2008) Application no. 54934/00 and Malone v UK Application no. 8691/79. In *Malone* the court held that 'the law had to be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and conditions on which public authorities are empowered to resort to…secret and potentially dangerous interference with the right to respect for private life and correspondence'. In *Weber*, the court also considered that minimum safeguards in relation to the exercise of state surveillance powers should include the 'nature of the offences' likely to give rise to intrusive surveillance activities.

proportionate, individuals exercising fundamental rights will not have adequate protection from arbitrary state actions.

Sufficiently clear and accessible

7. The scope of state powers in relation to the surveillance of political protest is neither clear nor accessible. The Bill enables policing bodies to carry out the activities of equipment interference and interception of communications for the purpose of the prevention and detection of *serious crime*. However, the definition of *serious crime* adopted for the purposes of the Bill potentially encompasses protest activity that includes only *minor* criminality.

8. The Bill adopts the definition of serious crime used in RIPA 2000. It includes conduct (which would constitute one or more criminal offences) that:

    8.1.1. '…involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose[1016]'.

9. The effect of this provision is that it applies to any protest activity where some form of criminality is conducted by a 'large number of persons' with 'common purpose'. This appears to create a lower threshold for the use of state surveillance in the context of mass protest - on this basis, *any* criminal activity, no matter how minor, which is conducted by a large number of people falls into the category of *serious crime*.

10. The scope of the statutory purpose of *preventing and detecting serious crime* is therefore highly uncertain. Does *serious crime* include, for example, a university occupation by students, or a mass protest in a quasi-public place such as a privately run shopping mall, protests which may include offences of aggravated trespass by virtue of them taking place on private land? Does it include environmental protests, such as those taking place around the country in opposition to hydraulic fracturing which have frequently featured arrests for obstruction of the highway?

11. We suggest that these provisions are not compatible with the ECHR, and that there is an urgent need to ensure that interception of communications and equipment interference are genuinely restricted to the prevention and detection of serious offences.

12. We have additional concerns about the use of communications data in relation to public protest and political activism. The lower threshold of preventing and detecting *crime* provides significant operational discretion to the authorities in relation to protest activity. We are concerned that monitoring of such data in relation to protest activity will become routine, justified by a wide and generalised interpretation of the need to *prevent crime*.

13. We suggest that any interference with protest activities on the part of the state should have a higher threshold than the broad purpose of the *prevention of crime*.

Necessity, proportionality and law enforcement discretion

14. The scope of surveillance activities are, of course, further limited by the requirements of necessity and proportionality. However, in the absence of further guidance on the

[1016] In 2000 Liberty warned that this definition 'extend[ed] the net of surveillance indiscriminately to participants in legitimate collective activity - industrial action, organised protest and so on - who are not themselves suspected of inherently serious wrongdoing.' We would agree with that assessment.

circumstances in which surveillance may be necessary and proportionate in the context of public protest, we do not consider this to be adequate protection.

15. Law enforcement bodies retain significant operational discretion in assessing the proportionality and necessity of surveillance operations, and it is not clear that oversight bodies will have either the capacity or capability to challenge operational decision making. The role of oversight bodies appears to be largely focused on procedural issues and in considering whether there is a 'less intrusive' means of obtaining information.

16. The track record of specialist policing bodies in acting proportionately in relation to the surveillance of protest is not reassuring. The lead is taken by the National Domestic Extremism and Disorder Intelligence Unit (NDEDIU), previously the National Public Order Intelligence Unit (NPOIU). The activities of this unit and its predecessors in authorising the deployment of undercover police officers within protest groups has been the subject of several reviews and is currently under examination by a public inquiry.

17. We are further concerned by the approach taken by the NDEDIU to the classification of 'domestic extremism'. While claiming to have tightened up the definition of domestic extremism in response to criticism by HMIC in 2012, Netpol has evidence that the categorisation continues to be applied to single issue protest groups that engage in low-level criminality, including anti-fracking protest groups which adopt peaceful (albeit sometimes unlawful) methods of protest.

18. We are therefore concerned that surveillance may be operationally justified against a wide range of protest groups on the basis that it is necessary (and proportionate) to the need to challenge 'domestic extremism'. Given that protesters and protest groups are unlikely to be able to challenge such classification, this may lead to the excessive and arbitrary use of state powers.

19. We suggest that there needs to be a much clearer indication of what may be considered to be 'necessary and proportionate' surveillance of activities protected by Article 10 and 11.

Thematic warrants

20. We have particular concerns relating to the availability of thematic warrants to law enforcement agencies. The Bill enables police units to obtain targeted warrants relating to:

    20.1.1. '…a group of persons who share a common purpose or who carry on, or may carry on, a particular activity.'

21. In the context of protest policing, this extends the use of surveillance activities to any individual associated with a protest groups that meets the definitions discussed above. Not only does the surveillance extend to individuals themselves engaging in (possibly low-level) criminal activity, it arbitrarily extends it to all individuals believed to share a 'common purpose' with them.

22. This provides policing bodies with wide-sweeping powers to undertake surveillance on political activists and protest groups. We suggest that this cannot be compliant with ECHR, nor acceptable in any democratic society.

Netpol

21 December 2015

New America's Open Technology Institute—written evidence (IPB0086)

1. New America's Open Technology Institute (OTI) is pleased to submit the following comments to the Draft Investigatory Powers Bill Joint Committee regarding the Draft Investigatory Powers Bill.[1017] New America's Open Technology Institute ("OTI") is a program of New America dedicated to technology policy and technology development in support of digital rights, social justice, and universal access to open communications networks. OTI, through its unique blend of policy expertise, technical capacity, and field-level engagement, seeks to promote a stronger and more open Internet to support stronger and more open communities. Digital Fourth Amendment policy and law is a particular area of interest for OTI, and the Institute testifies before the United States Congress regularly on issues of digital privacy and surveillance. New America is a non-profit civic enterprise dedicated to the renewal of American politics, prosperity, and purpose in the digital age through big ideas, technological innovation, next generation politics, and creative engagement with broad audiences.

2. We believe the measures proposed could create significant risks to privacy, security, and innovation, and should be approached with caution. Our comments focus on the bill's consideration of computer and network exploitation (CNE) as a response to "the loss of intelligence that may no longer be obtained through other techniques, such as interception, as a result of sophisticated encryption."[1018] We believe that if CNE is to be used, it must be limited, and should only be authorized – if at all – in narrow circumstances with strong protections. Further, we believe that certain measures under consideration – specifically, use of CNE for bulk collection and adding new vulnerabilities in software updates – should be completely prohibited.

I. Encryption is a net positive for security of both private data and the network as a whole.

3. Encryption is a vital resource that protects the information of individuals, corporations and governments from a variety of criminals and others who would do harm. It has done so for over thirty years. As the Open Technology Institute noted in a policy paper on the history of encryption, in the 1980's "commercial demand for encryption products exploded," and in 1991 PGP – a major practical tool for end-to-end public key encryption of files and e-mail that is still popular today – was publically released.[1019]

4. As end-to-end encryption of electronic communications has been available to the public for the last quarter century, neither the technology nor the challenges law enforcement may face regarding interception are novel. The most significant shift regarding encryption in recent years has been its growing value for average

[1017] Secretary for the Home Department, *Draft Investigatory Powers Bill* (November 2015), *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf, *hereafter*, *Draft Investigatory Powers Bill*.
[1018] *Draft Investigatory Powers Bill*, 16.
[1019] Danielle Kehl et al, New America's Open Technology Institute, *Doomed to Repeat History? Lessons From the Crypto Wars of the 1990's* (June 2015), *available at* https://static.newamerica.org/attachments/3407-doomed-to-repeat-history-lessons-from-the-crypto-wars-of-the-1990s/OTI_Crypto_Wars_History.abe6caa19cbc40de842e01c28a028418.pdf.

individuals and ordinary businesses as more and more data is stored and transmitted digitally, which is an argument against rather than for government interference in the technology.[1020] Given that encryption is an indispensable tool that is widely available to and used by law-abiding individuals, companies, governments, and non-governmental organizations across the world to protect their security in an increasingly hostile digital ecosystem, the Investigatory Powers Bill should explicitly disclaim any effort to prohibit or interfere with the development or use of encryption.[1021]

II. Any use of CNE should be narrowly tailored and only used a means of last resort.

5. Considering the expanded use of encryption and other security features by a wider variety of people and entities, governments may seek new methods to obtain evidence that they believe they can obtain in no other way. The draft bill clearly considers CNE to be one appropriate course in the face of these challenges. However, because CNE raises unique concerns regarding security, privacy, and accountability that are even more serious than those raised by traditional methods of interception, CNE – if used at all – should be subject to the highest legal standards and strictest checks and balances.

6. CNE is a threat to privacy because it is generally accomplished through unilateral and surreptitious action. When police use interception techniques that involve compelled assistance from a company, there is an independent party with the ability to object to surveillance that is overbroad or improper. CNE has no such third-party check on its use. In addition, by virtue of granting access to devices or networks that can transmit or store absolutely massive amounts of data unlike anything available in the physical world, CNE has the potential to return extraordinary troves of highly personal data to authorities on an unprecedented scale. The Supreme Court of the United States recently had to tackle the privacy implications of mobile phones, and said that "cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person… They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[1022] Even our smallest devices contain huge amounts of personal data, yet the CNE contemplated in the bill would yield much more, authorizing access to much larger systems and networks used by countless ordinary people.

[1020] For a comprehensive review of OTI's arguments against government mandates regarding encryption, please see *Read This Before You Rail Against Encryption*, New America Weekly, Nov. 19, 2015, *available at* https://www.newamerica.org/weekly/read-this-before-you-rail-against-encryption/.

[1021] Home Secretary Theresa May has stated that the bill "will not ban encryption or do anything to undermine the security of people's data.". *See*, The Associated Press, *Apple Boss Cook Says He'll Resist UK Government Spy Law Plan*, Nov 11, 2015, *available at* http://bigstory.ap.org/article/c176a081b3d9418e90aa788a52495fd7/apple-boss-cook-says-hell-resist-uk-government-spy-law-plan. However, some commentators fear that particular provisions of the bill would do just that. *See*, Alex Hern, The Guardian, *Tech Firms Warn Snooper's Charter Could End Strong Encryption in Britain*, Nov 9, 2015, *available at* http://www.theguardian.com/technology/2015/nov/09/tech-firms-snoopers-charter-end-strong-encryption-britain-ip-bill.

[1022] *Riley v. California*, 573 U.S. __ (2014).

7. CNE also raises security concerns because it necessarily involves the use of some sort of vulnerability in the software of the target's device, software that may also be used by thousands or even millions of others. Unfortunately, vulnerabilities don't care who uses them. Any vulnerability used by government in compliance with the law can also be used by bad actors for malicious purposes, be they identity thieves, fraudsters, corporate spies, or foreign intelligence operatives. Government should be in the business of making networks and devices more secure, and telling software vendors about the vulnerabilities it knows of so that they can be patched. Frequent reliance on CNE would undermine its motivation to do so and thereby leave those widespread vulnerabilities open to malicious actors. Furthermore, if the security of the government's storage or transmission of such stockpiled vulnerabilities were compromised, the government's use of CNE could even alert criminals and spies to vulnerabilities of which they were previously unaware.

8. Because of all these concerns, OTI has previously concluded when commenting on this issue in the United States that with CNE, "we are faced with a digital surveillance technique that is substantially more invasive than the analog electronic surveillance techniques of the past."[1023] If used at all, checks should exist to ensure that CNE is at most a measure of last resort, and that it does not become a commonly relied-upon investigative technique. CNE should therefore only be deployed with judicial authorization based on a strong factual showing, and only after the government has demonstrated that less intrusive means of obtaining the information have been exhausted. That authorization should also be coupled with strict time limits defining the duration of the surveillance and requiring minimization of data that is not responsive to the government's stated need as particularly described in the authorization.

9. Even with all of these checks, the use of CNE still carries a unique range of serious privacy and security risks that distinguish it from traditional surveillance and may make any use at all unreasonable. These risks include the privacy risk to non-suspects who share the target computer or network; the risk that the government's CNE software may spread to non-target computers or networks; the possibility, in cases of botnet investigations or so-called "watering hole" attacks, that thousands or even millions of computers may be infected; and the risk that the software used to remotely access any of those computers or networks may end up causing damage, either by altering or deleting data or creating brand new security vulnerabilities that may be exploited by others.[1024] All of these risks are amplified even further when the CNE is intended to enable bulk surveillance.

III. Bulk CNE would be profoundly dangerous to both privacy and security, and should be prohibited.

[1023] Testimony of Kevin Bankston on Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure, before the Judicial Conference Advisory Committee on Criminal Rules, at 3, Nov. 5, 2014, available at https://www.newamerica.org/downloads/OTI_Rule_41_Testimony_11-05-14_final.pdf.
[1024] See id. at 5-6.

10. Use of CNE against a large group of subjects is never appropriate, and would have severe harms for both privacy and security.

11. Bulk surveillance is in itself a controversial practice. By its nature this method does not distinguish between suspected bad actors and individuals with no connection to wrongdoing. Activities that involve such disproportionate impacts on privacy are unnecessary and unacceptable. In addition, debate in recent years has conclusively debunked the theory that bulk collection will provide unique value simply because it provides the government with more data, while also demonstrating the significant privacy risk posed by such collection.[1025]

12. Additionally, while we do not believe that bulk collection is necessary or called for, bulk collection of communications metadata (which is explicitly referenced in the draft bill[1026]) does not require the use of CNE. Communications metadata cannot be fully encrypted in the same manner as content or data at rest; in order for a third party to route data, information about the sender and recipient must be available. Such information, therefore, can generally be obtained from telecommunications providers when necessary and with the proper oversight.

13. Finally, use of CNE for bulk collection by definition requires exploitation of a vulnerability that impacts a wide population, and therefore represents a significant public security risk. As stated earlier, any vulnerability that governments can use can also be used by criminals or foreign governments, and one that targets a large number of people would be incredibly valuable to those other parties. Any time the government can engage in a bulk exploit, so might criminals, terrorists, or a foreign nations. Such a measure is bad policy, and can never "be necessary in the interests of national security."[1027] Instead, governments that obtain vulnerabilities that can be used on such a massive scale should inform the vendor of the software in question and encourage them to fix the vulnerability.[1028]

[1025] For example, the United States recently outlawed domestic bulk collection after the ongoing telephony metadata bulk collection program was deemed to provide no unique security value. According to the Privacy and Civil Liberties Oversight Board, there was not "a single instance involving a threat to the U.S. in which the telephone records program made a concrete difference in the outcome of a counterterrorism investigation [and] … no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack." The Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*, (23 January 2014), 11, available at http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf. *See also, Liberty and Security in a Changing World, Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies,* The President's Review Group on Intelligence and Communications Technologies, Dec. 12, 2013, 104 *and* Bailey Cahall, David Sterman, Emily Schneider, and Peter Bergen, *Do NSA's Bulk Surveillance Programs Stop Terrorists?,* New America, Jan 13, 2014.

[1026] *Draft Investigatory Powers Bill*, 20 ("Access to large volumes of data enables the security and intelligence agencies to piece together communications and other data and identify patterns of behaviour. This enables them to: Establish links between known subjects of interest, improving understanding of their behaviour and the connections they are making or the multiple communications methods they may be using").

[1027] *Id*, at 21.

[1028] *See*, Michael Daniel, *Heartbleed: Understanding When We Disclose Cyber Vulnerabilities*, White House Blog, Apr. 28, 2014 *available at* https://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities *and*

IV. Companies should never be forced to use update mechanisms to introduce vulnerabilities.

14. Government use of CNE should never consist of compelling a company to use a software update to introduce a vulnerability into an application or operating system. Use of software updates for CNE causes devices and software to be less secure. Such a method is even worse than leaving a known vulnerability unfixed, because rather than preserve an existing insecurity, it would involve government proactively weakening computer security, and increasing risk for consumers. And as with vulnerabilities left unfixed, vulnerabilities added through government action could be exploited by anyone who discovers them, including cyber criminals and other bad actors.

15. In addition to the direct security risks, this tactic would cause significant harm by discouraging good consumer behaviour. If it is possible that updates may actually make software less secure, individuals may decide they are better off leaving older versions of applications in place. Similarly, users may decide that automatic updates, which are widely viewed as vital for cybersecurity today, are more dangerous than not. Users should never question the legitimacy of software updates. Given cyber criminals' frequent use of older vulnerabilities for repeat attacks, and the importance of broad adoption of a patch when a mass vulnerability – such as Heartbleed – is discovered, it is critical that government does not discourage consumers from updating software.

16. Discouraging updates would cause problems beyond enhanced risk of cyber attack. Applications – especially those primarily designed for mobile use – are frequently updated to test or provide new features, and increase functionality. On average, the most popular iPhone applications are updated once every month.[1029] If large numbers of users ignore updates out of concern that they include government mandated vulnerabilities, it will undermine general innovation and development.

17. Thus even if government does not pursue a policy of requiring vulnerabilities be included in updates, the mere legal authorization and possibility that such action could occur would have major repercussions. To avoid these harms, any authorization for government use of CNE should make clear that compelled inclusion of vulnerabilities in updates is not permitted.

18. We hope these comments will assist the Science and Technology Committee in its evaluation of the Draft Investigatory Powers Bill. Please contact OTI Senior Counsel Ross Schulman[1030] if you have any questions.

21 December 2016

[1029] Hugh Kimura, SensorTower, *25 Top iOS Apps and Their Version Update Frequency* (15 April 2014), *available at* https://sensortower.com/blog/25-top-ios-apps-and-their-version-update-frequencies.
[1030] Available by email

News Media Association—written evidence (IPB0012)

The News Media Association is the voice of news media in the UK –whose national and local titles are read by 42 million adults every month in print and online. Newsbrands - national, regional and local newspapers in print and digital - are by far the biggest investors in news, accounting for more than two-thirds (69 per cent) of the total spend on news provision in the UK.

The NMA welcomes the Joint Committee's pre- legislative scrutiny of the Draft Investigatory Powers Bill and hopes that this will lead to substantial improvement of the Bill. The NMA is confining this submission to concerns relating to journalism. The NMA has also outlined these issues in its submission to the Joint Committee on Human Rights. The NMA also endorses the submission to the Inquiry by the Media Lawyers Association.

In our view, the draft Bill would not ensure adequate protection for freedom of expression as it does not provide sufficient substantive or procedural protections for press freedom wherever the investigatory powers could be brought to bear upon those pursuing journalistic activities, or journalistic material or the protection of journalistic sources. The Draft Bill would enshrine sweeping powers affecting journalist and their sources, leaving unchanged other RIPA surveillance powers used against the press.

Comprehensive and stronger safeguards than those provided by the current draft Bill for journalism and journalistic sources are necessary. Otherwise the relevant authorities will still be able to make unwarranted use of the powers relating to intrusive and covert surveillance under RIPA 2000 ss 26- 46 and all the powers governed by the draft Bill including interception of communications; obtaining of communications data and of equipment interference. These could be used for tracking individual journalists, investigative teams, the entire editorial staff of media organisations and the subject, progress, course and content of their investigations including outside sources and confidential sources. They allow identification of confidential sources, directly or indirectly; access to information constituting unpublished journalistic material, including confidential and indeed legally privileged material; equipment interference measures not only allow surveillance of journalists and the media , but convert them into unwitting state agents. Retention and analysis of data , such as the records of websites visited over a twelve month period would also help identify the subject and course of journalistic investigations. The provisions permit access, accumulation and sifting of journalistic information gathered, with the risk of its use or disclosure for other purposes. The Draft Bill would still allow the relevant authorities to evade satisfaction of the stringent tests necessary for proper safeguard of press freedom. It would also continue to permit the police to bypass the statutory protections that Parliament and the UK courts have laid down in the Police and Criminal Evidence Act 1984 (including media rights of notification and challenge, so recently rescued and safeguarded by Parliament in the Deregulation Act 2015) Terrorism Act 2000 and other legislation

The new legislation must provide robust statutory safeguards against state interference with journalism, and this must be set out in the primary legislation. At minimum, such safeguards should apply to any application for authorisation of any powers under RIPA 2000 or the new Investigatory Powers legislation, by any authority eligible to apply for and use such powers

in relation to the media and journalists, journalistic material and sources of journalistic material. These new safeguards should be akin to the PACE journalistic protections. They must be of wider application, contain essential procedural safeguards including prior media notification and challenge of applications before a judge, incorporate stronger conditions for grant of an application and include the right of swift media appeal. To safeguard press freedom and protect sources, there must be prior judicial consent , independent of politicians, to any application; any applicant must be required to disclose that the material might relate to journalists, journalistic material and journalistic sources, directly or indirectly, the media should have a statutory right to prior notification of any application for use of any of the RIPA or IP Bill powers together with details of the substance and the grounds for the application; the media must have the further right to contest the application before a judge; the applicant must meet stronger criteria and more stringent conditions for grant of the investigatory powers – such as the PACE provisions outlined below; the judge, with the benefit of hearing informed media contest of the applicant's case, must be satisfied that the applicant has fulfilled all the relevant conditions for grant of the application and that it is in the public interest to do so.

Under PACE, the applicant has to provide- and the media has the right to know and to contest- certain information to the court. The applicant must provide details of the serious offence and/or investigation, must specify the material sought, explain why such material would be of substantial value to the investigation by itself or in combination with other material, detail whether alternative ways of obtaining the material are available and whether they have been tried and most importantly, satisfy the judge that it is in the overall public interest that the application for the material or access should be given. The media has rights and route for swift appeal of orders granted. All these well established journalistic safeguards are absent from the draft IP Bill. Equivalent protections to these must be included in the final Bill.

Addition of such statutory safeguards to the Draft IP Bill would provide stronger and more comprehensive protection for freedom of expression relevant to journalistic investigation, reporting and publication, together with the protection of journalistic sources. We do not believe that this would delay, hinder or jeopardise any investigation. The PACE and Terrorism statutory procedures and conditions have been in operation for many years. Such additional protections could easily build upon the Draft IP Bill's proposals. For example, the Bill already specifies certain general safeguards or additional protective steps for other potential subjects, such as MPs.

Indeed, the draft Bill recognises that journalistic safeguards are necessary, but , aside from the inadequate protection of s 61, restricts this to guidance in statutory surveillance codes. Such codes have already proved ineffective in protecting journalists and their sources under the RIPA regime to date. Stronger protection is necessary.

We refer you to the MLA's summary of known use of RIPA powers against journalists working for local and national press. There must be no repetition of the disturbing case of Sally Murrer or other instances where those granting an application for use of powers were unaware of the journalistic dimension. Nor should the new system tolerate the absurdities of local authority covert surveillance of journalists in tea shops, or very worrying police

requisition of communications data, in order to try to trace the sources of leaks to local government or political correspondents. Nor should there be any perpetuation of the past regime of undisclosed applications and authorisations for unknown purposes for use against the media.

The Draft IP Bill does not provide extensive enough or strong enough safeguards for press freedom and protection of sources.

Clause 61 is the only specific journalistic provision in the Bill and provides limited protection. It is confined to interception of communications data and then only to applications with the purpose of identifying or confirming the identity of a journalist's source. It does not apply to all potential applicants and users of the powers (only the police – and they are not restricted to applications relating to the most serious crimes), nor to all categories of journalistic material that could identify journalistic sources, whether directly or incidentally, nor to all the journalistic material that is protected under PACE. It does not protect the media and its sources against the grant and use of the surviving RIPA covert and intrusive surveillance powers, nor against the grant and use of all the other powers under the Draft IP Bill such as interception of communications , or equipment interference, or retention and access to personal data records. These powers could also all result in the identification of sources and access to journalistic material, confidential or otherwise, with risk to the journalist, source and reporting freedoms. Clause 61 must be improved, but this must be in conjunction with the addition of other clauses introducing the PACE type press freedom protections and procedures necessary in relation to all applications and use of powers under the RIPA and IP legislation

The proposed codes relating to the exercise of the other powers under the Bill against journalists will not address media concerns. RIPA surveillance codes have proved inadequate protection to date. The combination of the proposed new Codes and the introduction of the Judicial Commissioner in section 61 and generally elsewhere as proposed in the Draft Bill will not provide the strong and comprehensive safeguards necessary for press freedom.

The role of the Judicial Commissioner does not allay media concerns. The Judicial Commissioner is only to apply 'the principles of judicial review' to Ministerial consent. This does not enable rigorous test of the applications' merit. The Minister and the Judicial Commissioner's evaluations will not benefit from hearing media challenge and contradiction of the applicants' assertions and/or of Ministerial acquiescence. Ministerial or judicial consideration, however careful, will not be informed by evidence and submissions, put forward by media organisations, or their legal representatives, or by any representatives on behalf of any who might be the subject of the powers to application . And while the applicant can challenge a refusal, the oblivious media organisation, journalist or indeed any other potential subject affected, cannot contest the application, the grant of consent, or review of a refusal, or even make a retrospective complaint. Moreover, urgency procedures allow the 'so called double lock' to be bypassed, even where it applies, so that the powers can be used and damage done long before the review deadline and any possible revoke. Nor can the oversight system remedy any harm caused by inadequate protection. The basic journalistic problems and sources' vulnerability will persist, as the draft Bill does not provide adequate protection for freedom of expression in relation to journalistic

activities and journalistic sources and journalistic material to the applicable standard. The police and others will still be able to evade the tougher PACE requirements where applicable, or use alternative powers, if easier.

The NMA submits that the Draft Investigatory Powers Bill requires review to remedy its current deficiencies of protection for press freedom, Substantive safeguards and procedural protections, akin to PACE must be introduced, in relation to all investigatory powers under RIPA and the new Act that could be deployed against the media.

13 December 2015

NSPCC—written evidence (IPB0049)

1. Access to communications data is recognised by the NSPCC as an essential part of modern policing: it is used in the vast majority of cases involving child abuse and exploitation, and also allows law enforcement to trace vulnerable individuals and provide assistance where safeguarding is needed.
2. Continued access to information that allows the police to identify individuals is an important part of ensuring that victims of abuse and exploitation are able to obtain justice, as well as locating vulnerable children where there are immediate concerns to life.
3. The draft Investigatory Powers Bill offers the legal frameworks that support necessary investigations where serious crimes have been committed, although the NSPCC would also emphasise that it is vital that the Bill grants access to communications data in instances where there is concern that a child's life is in danger or a child has disclosed abuse by a person in a position of trust. This submission is based on information drawn from research conducted by the NSPCC, as well as information and case studies from the National Crime Agency (NCA), and other law enforcement agencies (LEAs), about how digital evidence is used in the prosecution of abuse.
4. Four key areas form the basis of this response. These areas include:
    1. Is the retention of existing powers, granted under the Regulation of Investigatory Powers Act (RIPA) and the Data Retention and Investigatory Powers Act (DRIPA) necessary?
    2. Is the proposed extension of powers, to include Internet Connection Records (ICRs), proportionate and necessary?
    3. The value of intercepting and retaining communications data
    4. Improving police access and understanding of communications data

Key considerations for the NSPCC

1. Child abuse and exploitation often include an online or digital element, therefore it is vital that the police have the powers to pursue perpetrators in this arena.
2. Children, like adults, have a right to privacy.
3. In those instances where a child's life is in immediate danger, or when abuse and exploitation are suspected, it should be considered proportionate and necessary to access communications data.
4. Retention of communications data is particularly important in cases of abuse because disclosure of abuse of often a long, slow, and highly distressing process.
5. There is a compelling case for access to Internet Connection Records (ICRs) – this is pertinent to the NSPCC for two reasons:
    - It will support our helpline to safeguard children who are in immediate danger when they contact us online via mobile internet devices.
    - It is likely that it will improve law enforcement capacity to identify perpetrators and victims of abuse.
6. Improved access to communications data should be considered as one aspect of a broader journey to improve investigations into online abuse.

Is the retention of existing powers, granted under the Regulation of Investigatory Powers Act (RIPA) and the Data Retention and Investigatory Powers Act (DRIPA) necessary?

5. Existing case studies from the UK and Germany indicate that retention of and access to communications data continue to be a central aspect of actively pursuing and prosecuting cases of child abuse and exploitation. In the first nine months of 2015, the NCA used communications data to safeguard 399 children and arrest 682 individuals for making, distributing, and possessing indecent images of children.[1031] Likewise, the report *A Question of Trust* highlighted that new legislation in Germany, regarding the retention of communications data, has led to a deterioration of the capacity of German police to investigate online abuse and exploitation. During 'Operation Rescue' – an investigation that dismantled an international paedophile ring – British police made 121 arrests from 371 identified suspects. However, despite 377 referrals from the British police to German police, no arrests were made. This difference was attributed to the fact that Germany no longer retains metadata, thereby limiting avenues of investigation available to the police. The NSPCC would have substantial misgivings if data were not retained and the ability of the police to trace individuals involved in paedophile rings was impeded – as appears to have occurred in Germany.[1032]
6. Despite the numerous benefits that the internet offers young people, it is also the sad truth that it facilitates the sharing of indecent images of children, as well as encouraging the creation of new images. In 1990, the Home Office estimated that there were 7,000 indecent images of children; there are now millions of individual images that can be accessed through the internet and recent research suggests that the tone of these images has become increasingly violent and sadistic.[1033] Therefore, it is vital that law enforcement is able to pursue perpetrators through the channels whereby these crimes are committed. Without access to this online landscape, it will become increasingly difficult to tackle these prominent forms of abuse.
7. In an era where communication is dominated by various forms of social media (and the internet more broadly), social media has also become a central avenue for investigation. Technological innovation has given perpetrators new ways of accessing victims and new means through which indecent images can be shared. Therefore, it is necessary that policing capacity continues to reflect the realities of modern abuse; and to do this, the police will continue to require access to this form of digital evidence.

Is the proposed extension of powers, to include Internet Connection Records (ICRs), proportionate and necessary?

8. The NSPCC recognises that retention of ICRs would represent a notable expansion of existing information collection. However, existing evidence suggests that this is a necessary expansion of existing capabilities. Smart phones, and the growth of roaming internet access, has changed the ways that people access the internet, which has, in turn, affected how useful the information is when it is returned to investigating officers. From the perspective of those working to safeguard children, this raises two problems: the first is that, as children have begun to contact helplines via online channels (rather than via phone) it has become very difficult to trace vulnerable children whose lives are at risk. Over recent years, this has become even more important at 71% of our contacts

[1031] Figures drawn from the NCA and National Police Chiefs' Council briefing.
[1032] David Anderson Q.C., *A Question of Trust: Report of the Investigatory Powers Review*, June 2014, p. 262.
[1033] *A Picture of Abuse: A thematic assessment of the risk of contact sexual abuse by those that possess indecent images of children*, CEOP, June 2012.

are made online, and online counselling sessions are more likely to result in disclosure of immediate threat to life (for instance, suicidal feelings and a plan to act on them). The second problem, which emanates from changes in the way that most people access the internet, is that it has made it more difficult for officers investigating online abuse to pursue additional lines of investigation – such as pursuing additional perpetrators, and locating victims that have not yet been identified. Therefore, the NSPCC would support law enforcement's access to ICRs as proportionate in cases where a child's life is at risk, and in cases of abuse and exploitation.

9. Briefings from the NCA have demonstrated how roaming IP addresses have made differentiating between individual users difficult. The NSPCC is concerned that without the ability to trace the contacts between vulnerable children and helplines, it might become increasingly difficult for organisations to safeguard children who are at immediate risk. In instances where a child is at risk of immediate harm, accurate and timely responses are of the utmost importance. A smooth application process to access this information, which could facilitate the swift location of individual children, should be a priority in the creation of the framework that determines access to ICRs.
10. Of a sample of 6,025 cases relating to indecent images of children online, the NCA found that in 14% of these cases, access to ICRs would have enabled the identification of the perpetrator; without this information, it was not possible to identify the individual involved.[1034] Furthermore, within this sample, in 58% of these cases, a suspect had been identified but it had not been possible to identify other perpetrators that they had been in contact with, nor had they been able to identify other victims. As a result, these children are unlikely to have received the proper safeguarding or support. Any new powers regarding access to personal data should be mindful of the right to privacy, which also includes children's right to privacy; nevertheless, in cases where abuse is known or suspected and the safeguarding of children is at risk, the NSPCC would argue that this fulfils the requirement for access to be proportionate and necessary.

The value of intercepting and retaining communications data

11. Research by the NSPCC has shown that it can often take a long time for children to summon the courage to disclose abuse and this means that we need to continue to have access for a period of time to allow support an investigation (in fact, the average time taken to disclose is 7.8 years).[1035] Therefore, in cases of abuse, it is important that communications data remains available after the fact so that, where possible, investigations are able to draw upon this data. Without the retention of this data, it would become almost impossible to investigate allegations of online abuse as investigations are likely to occur retroactively, rather than through 'live' interception – which is more common in investigations for other crimes.
12. Dissemination of indecent images of children often occurs through vast, closed networks of individuals, and it is only once the illegal nature of these networks is uncovered that investigating police are able to begin piecing together the broader picture. Specific targeting of these groups would remain very difficult, as they tend to be hosted on legitimate sites that are unwittingly used to host or stream illegal content. Likewise, legitimate social networking sites are often used as a vehicle for grooming, as they offer

[1034] Figures drawn from the NCA and National Police Chiefs' Council briefing.

[1035] Debbie Allnock & Pam Miller, *No-one noticed, no-one heard: A study of disclosures of childhood abuse.* London: NSPCC, 2013.

the opportunity to contact with children and increasingly sexual abuse will occur without any physical contact actually occurring between the victim and perpetrator.[1036]

13. Therefore, mass collection of communications data offers a net through which these activities can be captured and, if necessary, investigated – should there be a clear reason to do so. In this regard, the NSPCC supports the mass collection of data, but only in so far as it allows for targeted access by law enforcement – once the requirements of rigorous safeguards for access to private information have been fulfilled. Only once a complaint has been made, and it has been deemed proportionate to access this information, should it be possible for investigating parties to track an individual's history or monitor traffic on websites that might be hosting illegal content.

Improving LEA access and understanding of communications data

14. The NSPCC welcomes any simplification of current legislation. Childline practitioners have suggested that there can often be confusion about what the police are able to do with communications data. It is not uncommon for referrals by practitioners reporting concerns about the immediate safety of a child to be met with a lack of knowledge about how communications data can be accessed or unaware that such functions are available to them. Clearer legal frameworks might help to improve understanding of the tools available to the police; nevertheless, it is also essential that law enforcement receive full training in this regard to facilitate smooth access to information, as and when appropriate.
15. Since 2010, the number of cases referred to the NCA from the National Centre for Missing Children (NCME), regarding indecent images of children shared via social networking sites and email, has increased by 275% and in the last year alone, it has increased by 25%.[1037] It is clear that this represents a significant investment of policing time and resources. Therefore it is essential that the legal framework is clearly outlined and understood by officers, to ensure that applications are conducted in a smooth and timely manner, and urgent action to safeguard children can be taken as required.
16. Children's social lives have become increasingly indistinguishable from their online lives; as a result, digital evidence is often a fundamental part of investigating and prosecuting cases of abuse and exploitation. *Online and on the edge: Real risks in a virtual world. An inspection of how forces deal with online sexual exploitation of children* by the HMIC demonstrated that only 55% of investigations were considered 'good' or 'adequate'. There were equally concerning findings that significant delays in the forensic analysis of digital devices by High Tech Crime Units were very common, with delays of 12 months not 'unusual'.[1038] Delays, insufficient training in the collation of digital evidence, and the lack of awareness of the legal processes to access communications data, have all been cited as barriers to improving such investigations.
17. Without improvements in this sphere of investigations, it is unlikely that these increased powers will, in and of themselves, improve the experience of children who report abuse. As a result, the NSPCC considers the draft Investigatory Powers Bill to be part of a broader set of changes required to improve policing capacity and to support the sophisticated investigatory practices that have become an established part of safeguarding children in both their online and offline worlds.

[1036] https://www.nspcc.org.uk/preventing-abuse/child-abuse-and-neglect/grooming/what-is-grooming/

[1037] Figures drawn from the NCA and National Police Chiefs' Council briefing.

[1038] *Online and on the edge: Real risks in a virtual world. An inspection of how forces deal with online sexual exploitation of children*, HMIC, July 2015, p. 24.

18. Improvements in the quality of investigations will not be achieved by amendments to the powers of police to access personal information alone: the technical skills and training for police forces to make use of these powers; staffing capacity to follow through on investigations; and greater awareness of the serious nature of online abuse, all need to be improved if we are to support children appropriately through investigations and prosecutions of abuse and exploitation.

18 December 2015

The Odysseus Trust—written evidence (IPB0030)

Introduction

1. The Odysseus Trust is a non-profit company limited by guarantee which seeks to promote good governance and the effective protection of human rights. The Trust is directed by Lord Lester of Herne Hill QC, who is assisted by his senior researcher Caroline Baker and Parliamentary Legal Officers, Clare Duffy and Zoe McCallum.

2. This document responds to the Call for Evidence made by Joint Committee on the Draft Investigatory Powers Bill ("the Bill"). It focuses on arrangements for the interception of communications subject to legal professional privilege (LPP), in response to the second of the Committee's thematic questions.

Summary

3. The Trust shares the view of the Bar Council and Law Society that

    - There should be a statutory prohibition on the *deliberate* targeting of communications subject to LPP;
    - Where there are reasonable grounds for suspecting LPP is being abused, there must be a system of *prior judicial authorisation* (akin to the protection currently given to journalists' sources) for covert information-gathering; and
    - Codes of Practice must contain stringent safeguards to minimise damage where legally privileged information is *likely to be* obtained and minimise the risk of *accidentally* examining, using, disseminating to third parties, or retaining it.

4. The bill as currently worded falls short because

    - It authorises the interception of communications subject to LPP;
    - It treats LPP as less worthy of protection than either journalistic or parliamentary privilege;
    - It contains no statutory safeguards to protect against the deliberate targeting of LPP; and
    - Any additional safeguards to protect LPP are left to be spelt out in Codes of Practice which are restricted to the exercise of powers provided under Part 3, have not yet been made available for scrutiny, do not have legal force and can be changed by statutory instrument.

The importance of legal professional privilege

5. Legal professional privilege (LPP) is the right of an individual to consult a legal adviser in absolute confidence, knowing there is no risk that the information will become known to

a third party without the client's clear authority. It exists for the benefit of the client, not the lawyer, who has no right to waive LPP without the client's express agreement.

6. In view of the fundamental rights at stake, it is wholly inadequate that a detainee can avoid covert surveillance only by electing not to speak to his or her lawyer. Where fear of surveillance inhibits lawyer-client communication, the accuracy of legal advice is the casualty. Defence teams may never know about legitimate defences open to a defendant and would be unable to advance them at trial. Courts will adjudicate cases on a misleading or incomplete basis. Where LPP is inhibited, it is not just individual privacy that is affected but the administration of justice as a whole.

Why it is unnecessary to legislate for exceptions to LPP

7. LPP attaches only communications *genuinely* aimed at obtaining legal advice. Any communication between a lawyer and their client in furtherance of a criminal purpose, including terrorism, do not attract its protection[1039]. Where the authorities have reasonable grounds for suspecting that the privilege is being abused, they may obtain a warrant for interception without overriding LPP. It is therefore **unnecessary** to legislate for exceptions to enable the *deliberate* targeting of communications subject to LPP.

8. It is true that in 2009, the House of Lords held by a majority that RIPA authorised covert surveillance of legal consultations in exceptional circumstances[1040]. That decision was consistent with the European Convention of Human Rights, which has not expressly prohibited such surveillance. The Strasbourg Court has instead made clear that Article 8 of the Convention affords strengthened protection to exchanges between lawyers and their clients. The Court expects the same safeguards to be in place to protect individuals from arbitrary interference in cases of the surveillance of a legal consultation as it requires in other cases concerning the interception of communications[1041].

9. The decision in *Re McE* came as a surprise to many lawyers, as:

    - LPP has been protected as absolute privilege in common and statute law since at least the sixteenth century;
    - RIPA does not refer to LPP; and
    - Parliament never debated the issue during the passage of the legislation.

10. It is important to emphasise that the circumstances envisaged by the Law Lords were **truly** exceptional. Lord Carswell gave examples confined to grave and imminent threats – such as a terror attack or the killing of a child[1042]. Lord Phillips of Worth Matravers took the view that

[1039] This is known as the "iniquity exception", though it is more accurately described as a contrant on the scope of LPP. See for example s10(2) of the Police and Criminal Evidence Act 1984 ("items held with the intention of furthering a criminal privilege are not items subject to legal privilege").
[1040] *Re McE*[2009] 1 A.C. 908
[1041] At least insofar as these principles can be applied to the form of surveillance in question: *R.E v United Kingdom*, Application No 62498/11, 27 October 2015, §131. For those safeguards
[1042] Ibid, §102

> "Covert surveillance is of no value if those subject to it suspect that it may be taking place. If it is to take place in respect of consultations between solicitors and their clients in prison or the police station, it will be of no value unless this is such a rare occurrence that its possibility will not inhibit the frankness with which those in custody speak with their lawyers"[1043].

11. By inhibiting discussion between lawyer and client, any expansion of these rare circumstances would undermine the whole rationale for conducting surveillance of legally privileged communications. In addition, the necessarily secretive nature of interception makes difficult to win back public confidence once undermined. Even where surveillance powers are closely circumscribed, the chilling effect could easily be triggered.

12. It is noted that in evidence before the Committee on 30th November 2015, the government did not foresee circumstances in which it would seek intentionally to target communications subject to LPP. The sole reason given for interception was that "there may be situations in which people try to abuse the privileges available to them"[1044]. That response misunderstood the scope of LPP and overlooked the existence of the iniquity exception.

13. If the executive cannot foresee circumstances in which it would need to target legally privileged communications, it is surely simpler and safer to put this beyond doubt by inclusion of a prohibitory provision to this effect in the bill.

Comparison with parliamentary and journalistic privilege

14. In relation to interception and interference warrants, the bill provides (clause 16) for consultation with the Prime Minister as an additional requirement before authorisation is sought to intercept an MP's communications. Journalists' sources are protected by the additional requirement of judicial approval (clause 61). No equivalent statutory protection is offered in respect of communications subject to LPP. Instead, additional safeguards are left to be set out in Codes of Practice, which appear to be restricted to the exercise of powers provided under Part 3 (Schedule 6, clause 4), have not yet been made available for scrutiny, do not have legal force and can be changed by statutory instrument.

15. It is unclear why LPP is regarded as less worthy of protection than other forms of privilege. Parliamentary and journalistic privilege are vital to freedom of speech and the integrity of the democratic process. LPP is vital to the integrity of the judicial process and the right of any person suspected of wrongdoing to a fair hearing by an independent tribunal established by law. Curtailing parliamentary or journalistic privilege runs the risk of suffocating democracy. Curtailing legal professional privilege runs the risks of committing the innocent to prison, undermining the integrity of the judicial process and

[1043] Ibid, §51.
[1044] Paul Lincoln, in response to questioning by Lord Hart of Chiltern.

weakening public trust in the very system on which society depends as a substitute for violence and disorder.

The risk of interception information being mishandled

16. It is manifestly unfair if one party to litigation has the power to monitor the confidential communications of the other. The government's position is that even where an individual is in litigation with the state, public authorities can intercept lawyer-client communications without interfering with the right to a fair trial – as long as interception information is kept away from prosecutors. Yet abuses have been documented suggesting an obvious and serious danger of miscarriage of justice:

    - In 2011, the Court of Appeal struck down the convictions of 20 environmental protestors for aggravated trespass because the prosecution had not been open about the role of an undercover police officer, Mark Kennedy.[1045] Tasked with reporting on the proposed criminal activities of extreme left wing protestors, Kennedy had infiltrated various campaigns. He was present when protestors received legal advice about the risks associated with their plan to occupy a power station.

    - In April 2015, the Investigatory Powers Tribunal ordered GCHQ to destroy illegally intercepted communications between a Libyan rendition victim, Abdel Belhaj, and his lawyer.[1046] Belhaj is suing the UK government for alleged involvement in his rendition and torture, which made the breach of privilege particularly disquieting. In mishandling that data, GCHQ admitted it had broken its own rules and had broken the law.

Existing Codes of Practice

17. In March 2015, the government amended the Acquisition and Disclosure of Communications Data Code of Practice to protect journalistic privilege. For the first time, the Code provided that law enforcement applications to find the source of information given to a journalist must not be granted without prior judicial approval. In light of evidence in the public domain at that time relating to failures by public authorities in the handling of *legally* privileged material, it is regrettable that the government did not take this opportunity to strengthen the protection of communications subject to LPP.

18. In February 2015, the Coalition consulted on two draft Codes of Practice relating to interception of communications and equipment interference, pursuant to s. 71 RIPA. The Codes were amended and laid before Parliament on 4 November 2015[1047]. The powers they contain are not sufficiently circumscribed, not subject to adequate protection against abuse. The draft Codes:

    - Continue to permit LPP to be violated for investigatory purposes;

[1045] *R. v Barkshire* **[2011] EWCA Crim 1885.**

[1046] *Belhadj and Others v Security Service and Others* [2015] UKIP Trib 13_132–H.

[1047] At the time of writing, the Codes have not yet been approved by both Houses of Parliament.

- Authorise the interception of legally privileged communications in "exceptional circumstances" so broad as to include threats to limb as well as life;

- Give no assurance that the conditions for interception are confined to reasonable suspicion of *prospective* activity; and

- Provide that authorisation for intercepting communications subject to LPP will be at the discretion of the secretary of state, not an independent judge (unlike the position in relation to identification of journalists' sources).

Further, under s72(2) RIPA, there can be no criminal or civil sanctions against officials or ministers flouting the codes[1048].

19. Draft codes of practice to be issued pursuant to the Bill have yet to be published. However, Schedule 6, Clause 4 of the bill appears to confine the forthcoming Codes to the exercise of powers provided under Part 3 (relating to communications data), excluding interception and equipment interference. It is crucial that Codes of Practice relate the exercise of **any** surveillance powers that may result in the acquisition of legally privileged material. The Codes must contain stringent safeguards to minimise the damage where legally privileged information is obtained; and safeguards to minimise the risk of examining, using, disseminating to third parties, or retaining it. At the very least, the Codes must comply with the requirements of the Convention as set out in a well-established line of authorities[1049]. There should be parity with the enhanced authorisation procedures and safeguards afforded to journalistic and parliamentary privilege.

Zoe McCallum
Anthony Lester QC (Lord Lester of Herne Hill)

17 December 2015

[1048] RIPA 2000, s72(2): A failure on the part of any person to comply with any provision of a code of practice for the time being in force under section 71 shall not of itself render him liable to any criminal or civil proceedings.
[1049] *Weber and Saravia v Germany* (2008) 46 E.H.R.R. SE5*; Kennedy v United Kingdom* (2011) 52 E.H.R.R. 4; *Uzun v Germany* (2011) 53 E.H.R.R. 24*; Michaud v France* (2014) 59 E.H.R.R. 9*; R.E v United Kingdom* (2015) App No 62498/11.

Ofcom—written evidence (IPB0129)

Summary

1. The Office of Communications ("Ofcom") is the UK's communications regulator. We were established in 2002, and our powers and duties are set out in the Communications Act 2003 and a number of other statutes. We have a range of duties set out in legislation to regulate telecommunications, the airwaves used for wireless communications and broadcasting, postal services and certain broadcasting matters. We also have powers to enforce general competition and consumer law. A number of our powers and duties reflect the UK implementation of EU law requirements.

2. Our main duties as regulator are to further the interests of citizens in relation to communications matters and to further the interests of consumers in relevant markets, where appropriate by promoting competition.

3. As the communications regulator, Ofcom is arguably in a unique position in relation to the draft Investigatory Powers Bill. As sectoral regulator, we have a number of duties to promote competition, protect consumers, report on the capacity of the UK's broadband and telephony infrastructure and other matters. In order to carry out these functions, we have a range of statutory information gathering powers which we use – whether consensually, or through the exercise of our formal information-gathering powers – to acquire information from communications providers.

4. These powers are not, with some exceptions, relating to those working in unlicensed pirate radio stations, for example – directed at the investigation of individuals, but at carrying out our duties to regulate telecommunications providers and services. Often in cases where communications data relating to individuals is acquired, we are acting on complaints and requests to investigate made by those individuals: for example, where they make complaints relating to nuisance calls.

5. We also have limited interception powers relating to our responsibilities to manage the UK's spectrum – the airwaves over which many telecommunications operate. Ofcom's spectrum engineers use these powers mainly to perform our statutory duty to investigate complaints of electromagnetic interference to spectrum users (anyone from mobile phone users to the emergency and air traffic control services). They may also be used in law enforcement (for example, to identify and prevent illegal uses of spectrum in ways which interfere with business or public services).

6. A number of our powers reflect requirements imposed on the UK in EU law for the purposes of telecoms regulation. They are subject to safeguards in the specific legislation from which they are derived. In general, they are used to protect citizens' and consumers' interests, rather than to investigate them: in particular, to investigate breaches of regulatory requirements by providers of services (corporate entities electing to undertake regulated activities).

7. Because of the nature of our role as regulator, there is potential for the Bill to very significantly affect the way in which Ofcom carries out much of its day-to-day work. This memorandum for the Committee therefore explains our powers and duties, their

origins, what our powers are used for and how often. It also explains the potential effects if the Bill were to remove or adjust Ofcom's powers or the arrangements for their operation. We would be very happy to assist the Committee further in setting out more detail in relation to any of these functions.

8. We understand the objective the Bill sets out to consolidate the powers authorities use for a range of investigative purposes. We also welcome the intention reflected in the current draft Bill to preserve the powers Ofcom (and others) use to perform sector-specific regulatory functions (clause 9, in particular).

9. Ofcom understands that this reflects a wish on the part of Government to preserve our existing regulatory functions and powers. Were the Bill to change those, it would affect, and may remove, our ability to perform the duties Parliament has given us. It could also breach the UK's EU law obligations. We think that would be unintended and clearly undesirable.

Introduction

1. Ofcom is the UK's National Regulatory Authority ("NRA") for telecommunications. We were established by statute (The Office of Communications Act 2002) and have a number of statutory duties and powers given to us by Parliament (in particular, by the Communications Act 2003). Many of these implement obligations placed on the UK by EU law (including the obligation under the EU telecommunications framework legislation to have a designated regulatory authority with certain objectives, functions and powers).

2. We regulate the electronic communications services, like fixed line and mobile services (telephone calls and broadband), the airwaves (the radio or electromagnetic spectrum) over which wireless devices operate, postal services and TV and radio broadcasting services. We also enforce general competition and consumer protection laws in these areas.

3. We are a sector-specific economic regulator. We have two overriding objectives, set out in the Communications Act 2003:

- to further the interests of citizens in relation to communications matters; and
- to further the interests of consumers in relevant markets, where appropriate by promoting competition.

4. To deliver the objectives set for us by Parliament, we exercise a range of powers and duties. We have some powers to gather information as part of performing our duties. These are described further below.

The draft Investigatory Powers Bill

5. Ofcom understands that the draft Investigatory Powers Bill is intended to set out a single comprehensive statutory framework for the powers that investigatory and public authorities have to intercept communications and to require

telecommunications and postal operators to provide communications data. It sets out the purposes for which those powers may be exercised and the procedural requirements and safeguards that apply.

6. We understand that the principal concerns intended to be addressed by the draft Bill are that:

- law enforcement and security and intelligence agencies have the powers they need to investigate serious criminality, including terrorist threats, in the digital age;
- those powers are clear and understandable; and
- there is appropriate oversight which balances the public interests in law enforcement and the protection of individual privacy.

7. In this context, Ofcom, which has some limited powers to intercept communications and to acquire communications data (for the limited purposes described in more detail below), is what David Anderson QC described as "a minor user" of these types of powers. In general, we use them to perform our statutory, sector-specific regulatory duties to protect citizens and investigate corporate entities undertaking regulated activities, rather than to investigate the conduct of individual citizens and consumers.

8. In the course of Government's preparation of the draft Bill, we have had a number of discussions with officials at both the Department for Culture, Media and Sport and the Home Office to ensure that Government is aware of the potential effects on Ofcom's ability to perform its statutory regulatory duties if the Bill changes or removes our powers (and those of co-regulators operating with our statutory approval), and is able to take account of that in preparing its proposals for scrutiny and consideration by Parliament.

9. The draft Bill published for pre-legislative scrutiny broadly seeks to preserve the existing scope of Ofcom's powers, and those of our co-regulators. It does so on the basis that these powers are required for the purpose of exercising our statutory regulatory duties and are subject to an existing series of statutory safeguards relating not just to personal data, but also to proportionality in terms of the burden on the industries that we regulate.

10. This is reflected, in particular, in clauses 5, 9 and 36 of the Bill. In broad terms, clauses 5 and 9 of the Bill preserve the operation of information gathering powers in other statutes which may be used by Ofcom to acquire communications data as part of the exercise of our regulatory functions. Clause 36 preserves Ofcom's existing power, currently in the Wireless Telegraphy Act 2006, to intercept communications for certain things we do as part of our duty to manage the radio spectrum - for example, preventing interference to users including key public services like Air Traffic Control and the police, ambulance and fire services.

11. Ofcom considers that the preservation of our existing powers enables us to fulfil our statutory duties without detracting from the main aims of the draft Bill. Removing or

amending those powers would risk impairing, or potentially removing, our ability to perform the duties Parliament has given us. In some cases could also put the UK in breach of its EU law obligations.

12. In order to assist the Committee's consideration of the approach taken in the draft Bill, and the above points in particular, the remainder of this evidence sets out in more detail:

- the powers we use to perform our regulatory duties and their legal bases;
- what safeguards and oversight are currently provided for in our use of those powers;
- what we use the powers for, and how often we do so; and
- the potential consequences for our ability to perform our functions as sectoral regulator if we were unable to use those powers (in terms of the inability to perform our duties and of the UK breaching EU law requirements).

Ofcom

13. EU Directive 2002/21/EC (commonly known as the "Framework Directive") requires member states to establish NRAs for telecommunications. This Directive is part of a common regulatory framework for electronic communications networks and services in EU law. That framework also requires member states to give NRAs a number of duties and powers, including information gathering powers.

14. Ofcom was established as the UK's NRA by the Office of Communications Act 2002. Our powers and duties are in a number of Acts of Parliament, including:

- the Communications Act 2003;
- the Postal Services Act 2011;
- the Wireless Telegraphy Act 2006;
- the Competition Act 1998;
- the Enterprise Act 2002; and
- the Consumer Rights Act 2015.

15. Ofcom's main statutory duties and functions include:

- furthering the interests of citizens and of consumers, where appropriate by promoting competition (under section 3 Communications Act 2003);
- ensuring the maintenance of a universal postal service (six days a week, with a universally priced delivery and collection service across the country) (section 29 Postal Services Act 2011);

- ensuring the radio spectrum is used in the most effective way (section 3 Communications Act 2003 and section 3 Wireless Telegraphy Act 2006);
- making and enforcing regulatory conditions under which telecommunications operators provide services (Articles 1-6 and 10 of the Authorisation Directive which is part of the EU common regulatory framework, and sections 45-63 and 94-104 Communications Act 2003);
- resolving disputes between undertakings about regulatory obligations imposed under the EU framework and national telecoms legislation (Article 19 Framework Directive, and sections 185-191 Communications Act 2003);
- enforcing legislation prohibiting nuisance telephone calls (under sections 128-130 Communications Act 2003 and the Privacy and Electronic Communications (EC Directive) Regulations 2003);
- stopping mobile phone network operators making excessive roaming charges (for using mobile phones abroad) (regulations 1 – 5 Mobile Roaming (European Communities) Regulations 2007));
- making and enforcing regulatory conditions for postal operators under sections 42 and 51 of the Postal Services Act 2011;
- allocating rights and licences to use the radio spectrum (Article 5 – 7 Authorisation Directive and section 8 Wireless Telegraphy Act 2006);
- investigating complaints of interference to spectrum users (section 4 Wireless Telegraphy Act 2006);
- investigating and prosecuting a number of spectrum-related criminal offences, like pirate radio broadcasting (sections 8 and 35 Wireless Telegraphy Act 2006);
- investigating and determining breaches of competition law under the Competition Act 1998; and
- enforcing consumer law under Part 8 Enterprise Act 2002.

16. We also have duties to regulate premium rate telephone services under sections 120-124 Communications Act 2003. Under those sections we have approved a co-regulator, PhonepayPlus, to operate a system of regulation of those services under its Code of Practice.

17. In performing these duties and functions, Ofcom has powers to require the provision of information, including from telecommunications and postal operators. The information may include communications data as defined in the draft Bill (very broadly, the who, how, when, where and with whom of individual communications). The powers include:

- section 135 Communications Act 2003 (information required in connection with making and enforcing regulatory conditions);

- section 136 Communications Act 2003 (information required for statistical purposes);
- section 191 Communications Act 2003 (information required for dispute resolution);
- regulation 2B Roaming Regulations;
- section 55 and Schedule 8 of the Postal Services Act 2011 (used to gather information for the purpose of enforcing postal regulatory conditions);
- section 32A Wireless Telegraphy Act 2006 (information relating to radio spectrum functions);
- section 26 Competition Act 1998 (information relating to investigating breaches of competition law); and
- schedule 5 Consumer Rights Act 2015 (information relating to consumer law enforcement under Part 8 Enterprise Act 2002).

There are also information gathering powers in the PhonepayPlus Code of Practice for regulating premium rate services, that Ofcom has approved under sections 120-124 of the Communications Act 2003.

18. Ofcom also has limited powers relating to the interception of communications for the purposes of our spectrum management duties (granting licences, preventing interference and investigating spectrum-related criminal offences). These are in sections 48 and 49 of the Wireless Telegraphy Act 2006.

19. A common feature of these powers is that they are subject to safeguards in the relevant legislation. For example, the Communications Act 2003 sets out (in section 137) that Ofcom may only require the provision of information by a telecommunications operator under section 135:

- for specified and limited regulatory purposes (such as investigating a regulatory condition we have reason to believe may have been breached);
- where we set out in a written notice the information required and the reasons for requiring it; and
- if the information required is proportionate to the use to which it will be put.

20. The nature of Ofcom's duties also limits the way the powers are used and the effects they have. The information gathering powers, for example, are used to acquire information from, and to regulate the conduct of, undertakings (usually corporate entities) which have chosen to undertake regulated business activities – as supposed to the investigation of individuals. The information obtained may relate to individuals, but their identities and conduct will be incidental to, not the subject of, Ofcom's regulatory activities. The aim of what Ofcom does is to further citizens' and consumers' interests, not to investigate them. We would, for example, gather data showing the line speed of each broadband line in the UK; billing information to

establish if a firm is unfairly charging its customers or about nuisance calls made by call centres.

Relationship with the draft IP Bill

21. In general, the draft IP Bill preserves the above powers. As previously noted, clauses 5 and 9 preserve information gathering powers in other statutes, which may be used to acquire communications data, where they are used for our regulatory functions. Clause 36 preserves Ofcom's existing interception power where used as part of our radio spectrum management duty.

22. Without these clauses, Ofcom would not be able to exercise a number of these powers. This is because, still speaking generally, they are civil regulatory powers. They are not, with one or two exceptions addressed below, powers that Ofcom exercises for purposes like preventing or detecting crime or protecting national security interests.

23. In the absence of clauses 5 and 9, therefore, the draft Bill would not provide a basis for Ofcom to acquire communications data from communications firms that we currently use to fulfil our regulatory duties. That would likely mean we would be unable to perform those duties in a number of cases and that the UK may be in breach of its EU obligations.

24. A similar point applies in relation to clause 36. The interception powers are a key part of the work our spectrum engineers do to protect spectrum users from interference.

25. The following examples illustrate these points. They set out how we use particular powers, how often we have done so, and what we think is the likely effect of not being able to exercise them. They also show why, in Ofcom's view, the preservation of these powers is necessary and appropriate.

26. There are also a small number of areas where the position of Ofcom's regulatory powers under the draft Bill is less clear. One is in relation to the powers of co-regulators, like PhonepayPlus, approved by Ofcom. Another is in relation to Ofcom's spectrum-related work on what are known as "White Space" devices (see further below). Ofcom's view is that the Bill should more clearly deal with the position in relation to these two matters.

Information gathering powers

Making and enforcing regulatory conditions

27. A key aspect of Ofcom's work is in making and enforcing the regulatory conditions under which telecommunications and postal operators operate. These cover a range of matters – there are 23 general regulatory conditions for telecommunications operators[1050], for example, which communications operators must comply with in order to offer services to consumers. They include a number of consumer protection

[1050] This is the term used in the draft Bill. In sectoral legislation and regulatory conditions, they are referred to as "Communications Providers." The terms are broadly synonymous.

rules, such as prohibitions of mis-selling, requirements to operate consumer complaints handling procedures and requirements to provide accurate bills.

28. Ofcom's powers to make and enforce these conditions come from Articles 1-6 and 10 of the EU Authorisation Directive, in particular. Article 10 requires that NRAs like Ofcom must monitor and supervise compliance with these conditions. These EU law requirements are implemented in sections 45 – 63 and 94 - 104 of the Communications Act 2003.

29. These duties and powers are supported by information gathering powers. Article 5 Framework Directive and Article 11 Authorisation Directive require that member states give NRAs powers to acquire information necessary to ensure compliance with the regulatory framework wherever objectively justified and proportionate. These requirements are implemented in UK law in sections 135 – 137 of the Communications Act 2003, in particular.

30. Section 135 Communications Act 2003, for example, enables Ofcom to require from certain persons, typically telecommunications operators, information we consider necessary for the purpose of carrying out our functions under Communications Act 2003 (like making and enforcing conditions). Safeguards are in section 137 (as set out above). Additional safeguards are in section 393 Communications Act 2003 which imposes a statutory prohibition on disclosing the information acquired.

31. Ofcom uses the information gathering powers as part of our work on a regular basis. We acquired information falling within the scope of the powers on over 250 occasions in 2014. The sorts of information we acquire using these powers includes evidence we use to make and enforce regulatory conditions, such as communications providers' internal procedural documents and records. The information we gather using this power may include communications data in any particular case. For example, information from individual customer accounts records, such as records of the services used and the bills charged. Of the over 250 cases in 2014, over 200 involved the provision of communications data.

32. The importance of this power and of Ofcom's ability to acquire communications data under can be demonstrated by reference to the enforcement of particular regulatory conditions. These examples also show how the powers are directed at fulfilling our duty to protect consumers, not to investigate them. Even where they involve acquiring communications data relating to individuals, our use of the powers is aimed at protecting them against the activities of regulated undertakings not at acquiring information on individuals' activities.

33. In 2011, for instance, we took action against a group of telecommunications companies for breaching General Condition 11, which requires telecommunications providers to levy accurate bills. This followed complaints of inaccurate billing from over 1,000 customers.

34. Using our powers under section 135 of the Communications Act 2003 we were able to acquire from the companies involved communications data about the extent to which consumers had used (or not) relevant services and the bills they received. 62,000 customers were affected by bills of between £1.3 and £1.7 million for services they

had not used. Our investigation enabled us to impose penalties of over £3 million on the companies involved.

35. Ofcom is currently undertaking an investigation into whether another telecommunications operator has inaccurately charged a significant number of customers. We have again used section 135 to acquire from it communications data about the extent to which customers have used and been charged for these services. Without the ability to acquire this data, Ofcom could not effectively enforce this key consumer protection rule.

Nuisance calls

36. We also use our information gathering powers under section 135 of the Communications Act to tackle nuisance calls. In particular, to take action against those making silent and abandoned calls, often made by call centres, which amount to persistent misuse of telephone services.

37. That kind of misuse is prohibited under section 128 of the Communications Act 2003, and sections 128 – 131 give Ofcom statutory powers to enforce that prohibition. Since tackling nuisance calls involves identifying the calling party, and the total number and nature of relevant calls that party has made to individual recipients, this use of section 135 again involves acquiring communications data under that power.

38. This is a key area of Ofcom's work to protect consumers. Evidence we gathered in 2015 suggested that 86% of consumers received unwanted calls on their landline over a four week period; with 60% receiving a silent call and an estimated 17% receiving an abandoned call.[1051] Our research in April 2015 suggested UK consumers received an average of 9.7 nuisance calls in a four week period.

39. The evidence also shows that 86% of silent calls and 82% of abandoned ones were considered annoying by recipients and 7 and 4% distressing. Ofcom received 25,450 consumer complaints about silent and abandoned calls in the 6 months to October 2015. They are also the issues that consumers complain about most to Ofcom.[1052]

40. Ofcom has used its powers in section 135 to enable it to take formal and informal enforcement action in relation to abandoned and silent calls twenty-six times in 2014 and 94 times in 2015. The use of these powers enabled Ofcom to take formal enforcement action to protect consumers against 18 companies, for which Ofcom imposed financial penalties totalling £2 million. We also took informal action, stopping or reducing the number of offending calls, in 76 cases between January and September 2015 with 17 cases still ongoing.[1053]

41. Again, our enforcement action in this area would have been significantly more difficult, quite likely not possible, were we unable to use the section 135 powers to acquire communications data from relevant telecommunications operators. That

[1051] Telecoms and Pay TV complaints Q3 2015, December 2015 http://stakeholders.ofcom.org.uk/binaries/research/telecoms-research/complaints/Q3_2015.pdf
[1052] ibid.
[1053] Telecoms Complaints Bulletin, November 2015 http://stakeholders.ofcom.org.uk/binaries/enforcement/telecoms-complaints-bulletin/Telecoms_Complaints_Bulletin_November_2015.pdf

would have left us unable to exercise the statutory powers Parliament gave us in this important area of consumer protection.

42. Ofcom also has powers, alongside the Information Commissioner's Office ("ICO"), to enforce the Privacy and Electronic Communications (EC Directive) Regulations 2003. Amongst other things, these prohibit unsolicited marketing calls to consumers who have registered with the Telephone Preference Service's ("TPS") 'do not call' list. Enforcement of these provisions is also likely to involve acquiring communications data and existing legislation gives Ofcom and the ICO powers to do so. For similar reasons to those above, Ofcom's view is that the draft Bill should similarly preserve these important powers.

Infrastructure reporting

43. Ofcom has a duty under section 134A of the Communications Act 2003 to publish reports on the communications networks and services provided in the UK. This report plays an important part in both identifying areas for Ofcom's and Government's policy focus and in giving businesses and consumers clear, accurate, easy to use information enabling them to make informed decisions about the services that can serve them best.

44. Preparing the report involves Ofcom using its information gathering powers under sections 135 and 136 of the Act to acquire information from telecommunications operators. That information is liable to include communications data such as the speed of each broadband line in the UK. Clause 9 of the draft Bill preserves the power to do that and Ofcom's view is that it is important it continues to do so, in order that we can effectively fulfil the duty imposed on us by section 134A.

Dispute Resolution

45. Another important area for Ofcom relates to regulatory disputes. Under sections 185 – 190 of the Communications Act 2003 Ofcom must resolve certain disputes about regulatory matters (for example, access to communications networks used to transmit calls) between telecommunications operators within a 4 month statutory deadline. Section 191 of the Act contains a power for Ofcom to acquire information to enable us to do so. These are powers and duties Ofcom is required to have by various parts of the EU regulatory framework.

46. The power in section 191 includes power to acquire communications data. Any particular dispute could require Ofcom to use that power to acquire that data and we have done so.

47. In one dispute, for example, we required copies of individual consumers' communications account information (bills) as evidence of whether the disputing telecommunications operators had transferred telephone lines without customers' consent. In another, about network access, we used the power to acquire records of individual calls being carried between disputing operators.

48. The Bill currently preserves this power (again, in clause 9). Were it removed, Ofcom would be unable to acquire the relevant communications data. We could not fulfil our statutory duty in relevant disputes, which could put the UK in breach of EU law.

Roaming Regulation

49. Ofcom also has powers to enforce the Mobile Roaming (European Communities) Regulations 2007 and obligations to resolve disputes between telecommunications operators under those regulations (which we must do within a statutory 4 month deadline). This legislation regulates the charges telecommunications operators can make for using their services abroad (roaming). Regulation 2B gives Ofcom powers to acquire all such information as we consider necessary for the purposes of our functions under the Regulations (and a counterpart EU Regulation).

50. Action Ofcom takes under these Regulations is likely necessarily to involve acquiring communications data, since investigations (into operators, and to protect consumers in relation to roaming charges) and disputes are likely to involve looking at the charges made for individual communications whilst roaming. Removal of this power – which is another currently preserved by clause 9 of the Bill – would risk inconsistency with the UK's EU law obligations (under the EU Mobile Roaming Regulation), as well as making consumers more vulnerable in relation to roaming charges.

Postal services

51. Ofcom also regulates postal services. We assumed these duties in October 2011. This followed the 2010 Hooper Report which recommended that under the new regulatory framework for postal services "the regulator must have enhanced statutory information gathering powers."[1054]

52. Ofcom's duties under the Postal Services Act 2011 include a duty to perform our regulatory functions in a way we consider will secure the provision of a universal postal service. Our functions include the making and enforcing of regulatory conditions under which postal service operators must operate.

53. Section 55 and Schedule 8 of the Postal Services Act 2011 enable Ofcom to require postal operators to provide us with "all such information" we consider necessary for carrying out any of our functions on postal services. They contain safeguards about the purposes for which information may be obtained and the form and proportionality of any demand for it. In any particular case, this may involve obtaining communications data and our view, accordingly, is that the draft Bill should preserve our power to do this, so that we can fulfil our statutory regulatory duties in relation to post. So far in 2015 we have issued one formal demand for information from 6 postal operators, for data about the volumes of parcels sent and about complaints made against them.

Spectrum Management

[1054] Saving the Royal Mail's universal postal service in the digital age, p.8 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/31808/10-1143-saving-royal-mail-universal-postal-service.pdf

54. As set out above, Ofcom has a legal duty to ensure the radio spectrum – the airwaves used by everyone from emergency and air traffic control services, taxi firms and boat owners, mobile-phone companies and broadcasters - is used in the most effective way. The Communications Act 2003 and the Wireless Telegraphy Act 2006 require Ofcom to secure "the optimal use for wireless telegraphy of the electro-magnetic spectrum"[1055] and "to provide a service consisting in the giving of advice and assistance to persons complaining of interference with wireless telegraphy."[1056]

55. Ofcom fulfils these duties by issuing licences to use the spectrum, exempting certain equipment and users from the need to hold a licence and by investigating complaints of interference.[1057]

56. Our spectrum management work includes matters as diverse as:

- responding to interference complaints from emergency service and air traffic control networks, where the interference may hamper the ability of the services to perform vital safety work;
- providing assistance to television viewers and radio listeners and mobile phone users whose use and enjoyment of services is affected by interference; and
- monitoring, where licences to use spectrum have been revoked, to investigate whether there is continued (and unlawful) activity by the previous licensee.

In 2014, for example, there were 262 cases in which Ofcom investigated interference to aviation in the UK and 1978 instances in which Ofcom investigated alleged continued activity by revoked licensees.

57. In order properly to fulfil our duties in these areas Ofcom needs to acquire relevant information. This would include communications data such as information about the location and nature of devices emitting signals. For that purpose, the Wireless Telegraphy Act 2006 gives Ofcom two relevant powers: (1) a limited power of interception provided for by section 49 of that Act; and (2) an information gathering power in section 32A.

Interception

58. The effect of section 49 of the Wireless Telegraphy Act 2006 is that Ofcom has powers to authorise certain staff to intercept communications for certain purposes. They are enabled to use wireless telegraphy apparatus to acquire information about the contents, sender or addressee of messages of which they are not an intended recipient.

[1055] Section 3(1), Communications Act 2003

[1056] Section 4, Wireless Telegraphy Act 2006

[1057] We also have powers to enforce various spectrum-related criminal offence, in respect of which, we think, the IP Bill provides appropriate interception and data gathering powers, and which are not, therefore, the subject of any more focus in this evidence.

59. Section 49 contains relevant safeguards. Ofcom staff may only be authorised to exercise the interception power where the authority is given in writing by a designated senior officer and only where the interception:

- is necessary on grounds such as national security, preventing or detecting crime or public safety; or
- is necessary for purposes connected with Ofcom's duties and functions under the Wireless Telegraphy Act 2006 (like investigating interference); and, in either case,
- the interception is proportionate to what it seeks to achieve (having taken into account whether the outcome could reasonably be achieved by other means).

60. Ofcom's spectrum engineering team of 30 engineers are authorised by our Director of Field Operations[1058] to exercise this power. They do so as part of Ofcom's duties to manage the spectrum and investigate interference and unlawful use as described above.

61. In particular, the engineers use the power to operate Direction Finding techniques and equipment to scan through the radio spectrum, to fix on interfering signals and to obtain their locations and identify their sources. They did so over 4800 times in 2014.

62. Without this sort of power, Ofcom would be unable, or unable without severe restriction, to investigate and manage spectrum interference, and unlawful use, effectively. That would present risks to the safety of life services and the everyday spectrum uses like mobile phone use and broadcasting which we protect from interference. It would also adversely affect our ability properly to manage and license spectrum users in a way that meet our duties relating to the efficient management and optimal use of the spectrum.

63. The current drafting of the Bill (clause 39) preserves these interception powers. Ofcom considers that necessary and appropriate for the reasons set out above.

Information gathering

64. Section 32A of the Wireless Telegraphy Act gives Ofcom a power to require those who set-up, install or use wireless telegraphy apparatus to provide us with information we consider necessary for the purpose of carrying out our radio spectrum functions. The power is subject to a number of safeguards. These include in section 32B of the Act that any requirement for information must be:

- in writing describing the required information and setting out OFCOM's reasons for requiring it; and
- proportionate to the use to which the information is to be put in carrying out our spectrum functions.

65. This is another information gathering power that Ofcom is required to be given by the EU framework (Article 10 of the Framework Directive, in particular). The information

[1058] Who is also our Director, Spectrum Engineering and Enforcement.

Ofcom may acquire using this power may include communications data. For example, information about locations from which signals are transmitted.

66. Were the Bill not to preserve this power (as it currently does in clause 9), Ofcom would be unable to acquire communications data from telecommunications operators for (non-criminal) regulatory purposes. This would undermine our ability to meet our statutory duties and put the UK at risk of breaching EU law requirements.

Areas for clarification

67. There are also certain matters in the Bill which, in Ofcom's view, would benefit from clarification. These concern the position:

- of co-regulatory authorities operating with statutory approval; and
- in relation to "TV White Space and the regulation of spectrum databases."

Co-regulatory authorities

68. As noted above, Ofcom has powers and duties in sections 120-124 of the Communications Act 2003 in relation to the regulation of premium rate services. In line with those provisions, Ofcom has approved PhonepayPlus, as a co-regulator, to regulate those services under its Code of Practice.

69. Premium rate services regulation plays an important consumer protection role. Such services have certain characteristics which contain the potential to harm consumers. They are easy to set up and shut down quickly, and individual transactions are relatively cheap (typically less than £10 and often much less) and easy to enter into. The value chain, however, can be complex – consumers pay their communications provider via charges on their phone bills, but the communications provider is typically not the provider of the premium rate service. Without effective regulation, these factors can enable unscrupulous operators to set-up schemes to harm consumers and evade detection.

70. Against that backdrop, the PhonepayPlus Code contains a number of substantive rules designed to protect consumers. They cover matters such as prohibitions on misleading sales techniques and ensuring consumers consent to transactions. These are supported by powers for PhonepayPlus to require regulated service providers to provide it with information (rule 4.2.3 of the Code of Practice).

71. The nature of the services and the rules in the Code mean that information PhonepayPlus acquires will often, if not almost invariably, include communications data. It is not, for example, possible to investigate complaints that a provider had charged consumers for services without their consent without acquiring data about consumers' accounts and the extent to which they had consented to, used and been charged for services.

72. Ofcom understands from PhonepayPlus that it investigated over 1900 cases in the financial years between 2012/13 and 2014/15 and that it acquired communications data in 99% of these. This enabled it to make formal adjudications in 41 cases in the

last of these financial years, for example, and to impose fines of £1.5m for breaches of its Code.

73. Without the power to obtain this data, it is unlikely PhonepayPlus could continue effectively to regulate premium rate services. Ofcom understands that the draft Bill does not aim nor intends to change systems of regulation and therefore suggests that it should make clear that the appropriate powers to acquire communications data for regulatory purposes are also preserved for statutory-approved co-regulators.

TV White Space and the regulation of spectrum databases

74. The committee has asked whether the wording in the draft Bill is sustainable in the light of rapidly evolving technologies and user behaviours and, overall, whether the Bill is future-proofed as it stands. One relevant area relates to our anticipated regulation of spectrum databases, specifically our work on "White Spaces."

White spaces

75. Government and Ofcom have worked together on a number of spectrum initiatives, which include the emergent and still developing area of White Space technology (more generally called, "Dynamic Spectrum Access"). This area of work stems from the significant value of spectrum to the economy and the UK's ambition to be a global leader in promoting new techniques that would enable the unlocking of greater value from it. The value of spectrum depends on how well it is managed.

76. One of the new approaches is the exploitation of White Spaces. "White Spaces" is a term to describe radio spectrum not being fully utilised in all locations all of the time. These gaps in spectrum usage can be shared with other users to deliver additional services, such as broadband access for rural communities and the development of local flood defence networks. The work Ofcom has done is part of our statutory duty to secure the optimal use of the spectrum.

77. Enabling access to white spaces makes it easier to exploit spectrum sharing opportunities but brings with it a high degree of complexity and challenges to the regulatory framework. In particular, the opportunistic nature of this type of spectrum access and the presence of other users in the same spectrum band, which results in the increased possibility of interference.

78. In February 2015, Ofcom announced its decision to allow authorisation of access to White Spaces in the UHF TV band (470 to 790 MHz) on a licence exempt basis, following a successful White Space pilot in 2014. In December 2015, Ofcom made regulations under the WT Act which will authorise the use of white space devices in TV White Spaces without the need to hold a licence from 31 December 2015. We expect the first devices to be introduced to the UK market during the course of 2016.

79. In order to access White Spaces, devices must connect over the internet to databases which have been qualified by Ofcom. These databases act as gateways to White Space spectrum by holding information on the frequencies available for sharing in different locations.

80. Devices must communicate with a qualified database and provide information about their technical characteristics and, in particular, their location (their device parameters), which databases then use to calculate and provide information to devices about the frequencies on which they may transmit and the power they may use (fig.1 below shows how the different parts of this framework interact together). In other words, the operation of the databases is likely to involve the transmission of communications data between the databases (and database operators) and White Space devices.

81. We have put in place a co-existence framework for access to TV White Spaces which should ensure a low probability of harmful interference. However, it is possible that interference may still arise to existing users of the spectrum band as a result of use of White Space devices. As part of our statutory duty, we intend to manage any reported complaints of interference in connection with White Space devices by using a web-based system we have developed in partnership with the databases.

82. Using that system, when we receive a complaint of interference from other spectrum users, we can acquire information about White Space devices active in a particular area and at a particular time from database operators as quickly as possible. That information is likely, as described above, to be communications data. We would acquire it with a view to establishing the cause of interference and seeking to resolve it as quickly as possible.

83. Being able to obtain (close to) real time access to information on White Space devices through such mechanisms will enable Ofcom effectively and promptly to deal with reports of interference in line with our statutory duty. We consider that it would become much more difficult to respond to complaints of interference efficiently and promptly if we did not have access to this information through such mechanisms. Furthermore, if we are not able rapidly to respond to and resolve interference, it may undermine confidence in dynamic spectrum technologies and make it more difficult to use this key spectrum sharing technology for other frequency bands in the future.

84. We have worked closely with spectrum databases to build in contractual and procedural safeguards to the processes by which we obtain and use information provided by them in response to interference. These are intended to ensure that requests for information are appropriately restricted in scope such that we only obtain information relating to use of White Space devices which is necessary for conducting our spectrum interference management activities.

The impact of the draft Bill

85. We would have concerns if the effect of the draft Bill significantly hinders our ability to manage interference caused by White Space devices, as this could have a detrimental impact on our ability to efficiently and effectively manage use of White Space spectrum.

86. We consider it likely that database operators would be telecommunications operators and that the information we would be obtaining from them on devices would be communications data, as those terms are currently defined in the draft Bill. On the basis of the potential for White Space devices to provide valuable exploitation of

unused parts of the radio spectrum, our submission is that the draft Bill should provide for Ofcom to be able to acquire that data from those operators. Without such a provision that value in the use of the relevant spectrum may not be exploited.

87. We intend to work with the Department for Culture, Media and Sports and the Home Office to clarify the implications of the draft Bill for management of White Space spectrum use, with a view to ensuring that we remain able to effectively and promptly manage interference in that context.

Other areas and future developments

88. Other areas that might be relevant in terms of future work and developments include regulation of certain kinds of online content and audience protection and of network security. Within the broad scope of our current duties, and quite possibly more so in future, Ofcom plays roles in relation to both.

89. On online content and audience protection, we have done work on the effectiveness of filters designed to protect minors from pornography. Further work on this – for example, regulatory action in relation to provision (or providers) of such content – may involve us acquiring information from telecommunications operators which falls within the definition of communications data.

90. We also have duties relating to network security. This could in future involve us in needing to acquire information relating, for example, to the sources of threats to that security, which would be communications data.

91. In both contexts, the preservation of regulatory powers to acquire communications data, which we may not be able to acquire under the draft Bill, would be a useful part of the regulatory armoury.

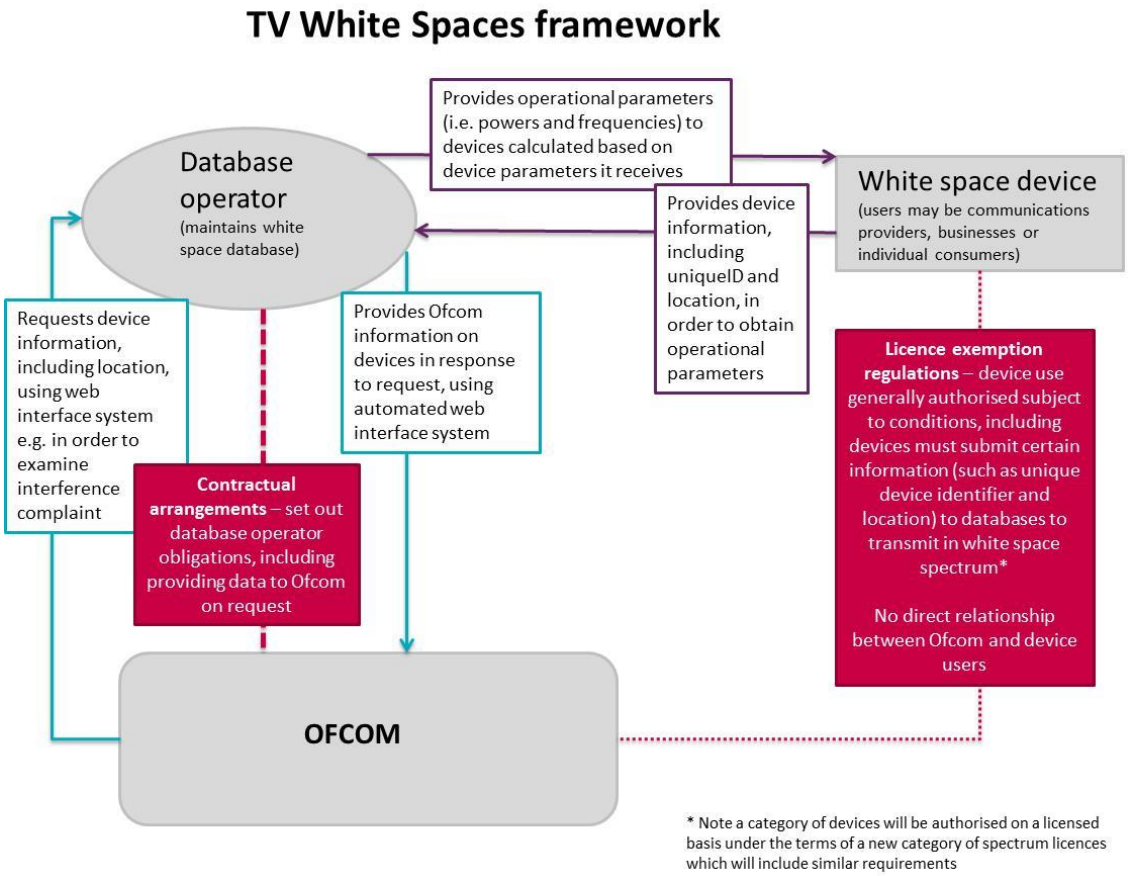

TV White Spaces framework
Provides operational parameters (i.e. powers and frequencies) to devices calculated based on device parameters it receives
Database operator
(maintains white space database)
White space device
(users may be communications providers, businesses or individual consumers)
Provides device information, including uniqueID and location, in order to obtain operational parameters
Requests device information, including location, using web interface system e.g. in order to examine interference complaint
Provides Ofcom information on devices in response to request, using automated web interface system
Contractual arrangements – set out database operator obligations, including providing data to Ofcom on request
Licence exemption regulations – device use generally authorised subject to conditions, including devices must submit certain information (such as unique device identifier and location) to databases to transmit in white space spectrum*
No direct relationship between Ofcom and device users
OFCOM
* Note a category of devices will be authorised on a licensed basis under the terms of a new category of spectrum licences which will include similar requirements

Figure 1

Open Intelligence—written evidence (IPB0066)

Introduction

[1] Open Intelligence is an independent think-tank operating at the intersection of technology and politics to advance security and liberty. Open Intelligence was founded by Andy Halsall and Loz Kaye.

Overarching / Thematic Questions

Necessity

[2] There is broad declared acceptance right from the security agencies to civil society groups that the country needs a new robust legal framework that meets our security needs effectively and that does not entail "browsing at will through the lives of innocent people"1059 as Andrew Parker has put it. This draft bill does not yet deliver on that ambition.

[3] The repeated case that has been advanced to the public in the past for broad powers, and to support the view that the chief intelligence threat is a lack of capabilities has been in the wake of serious incidents to assert that the incident proves the need for further capabilities. Several former Home Secretaries did this in the wake of the murder of Fusilier Lee Rigby for instance. However, the belated avowal of a range of powers, for example equipment interference in February 2015 and bulk powers under s.94 of the Telecommunications Act 1984 with the publishing of the bill show this case was presented to the public in a way that did not reflect the actual circumstances.

[4] In the wake of recent terror outrages it has been repeatedly the case that the perpetrators have been known to security agencies, the problem has not been gathering information, it has been what to do with it subsequently.

[5] The report on the intelligence relating to the murder of fusilier Lee Rigby details the collection of communications data, agent tasking, police liaison and further intrusive coverage of Michael Adebolajo in paragraphs 81 – 99. The conclusions focus on management and resource issues, the failures of the risk grading programme AMAZON (paragraph 49), the lack of assessing a cumulative picture from information available (paragraphs 144-148) , the organisational burdens of running IOCs (paragraph 258) , delays (conclusions Q, S, KK, LL) and issues of funding (conclusion DD).

[6] The conclusion must be that our national security is best served by focusing resources and improving practice, not pushing for the restatement and expansion of broad powers that have not been backed by a compelling case.

[1059] Andrew Parker interview http://www.bbc.co.uk/news/uk-34663929

[7] It is worth noting that even if the committee takes the view that the current threat scenario justifies broad powers for the SIAs, that is not the same as a case for restated and new powers for the Police, let alone any other bodies.

[8] In practical terms, the Danish experience with Internet session logging legislation shows not only has the case not been made for the broadest and significant new powers in the bill, they have been tried and found wanting. This is detailed in the Danish Ministry of Justice report document 5493311060. In section 6 the Danish intelligence agency PET as expected found targeted surveillance useful, but session logging only to a very limited extent relevant for investigations. Section 5.5.1.2 of the report detailed a range of problems encountered in terms of identifying individuals and resolving IP addresses, a declared aim of the IP Bill.

[9] The session logging law was subsequently dropped, and the Danish government was at pains to point out that this was not in response to the overturning of the EU directive following the Digital Rights Ireland case.

[10] The committee has heard that the government is intending something different to the Danish session logging law, without being informed how that is materially the case. Even so, the substantial problems that the Danes encountered showed that the devil was not in the details, but the overall conception and intention which is directly analogous to the IP bill. The report from the Danish Ministry of Justice shows the session logging legislation was flawed in necessity, proportionality and feasibility from the outset.

[11] Notably, the government is yet to make a case for the powers in the bill which convinces much of the tech industry and grassroots digital groups and activists. If the operation of this legislation is to function at all, it must have the support of those working, teaching and advocating in this sector. Apple CEO Tim Cook has voiced concern saying the draft bill would have “dire consequences” . The tech press has greeted the bill with headlines such as “How UK spies are about to take hold of the Internet” (Wired), “Snooper's Charter 'so technically complex' that it may be infeasible” (Ars Technica), “UK's super-cyber-snoop shopping list” (The Register). .

Legality

[12] In the case of Roman Zakharov v Russia the ECtHR1061 found unanimously that there had been a violation of Article 8 of the ECHR due to “arbitrary and abusive secret surveillance”. That the Russian SIAs and Police have “direct access, by technical means, to all mobile telephone communications” constitutes a particularly high risk. The Home Office may contend that the proposed safeguards are better than Russia's, but what is at issue is the actual practice. The first shortcoming the court identified that the lack of clarity about the categories of targets will serve as a warning for the wording of the bill. It is significant that the court found Mr Zakharov did not have to prove he was “even at risk of having his communications intercepted” to bring the case. This opens up a route to challenge all of the bulk provisions in the bill as it stands.

[1060]Redegørelse om diverse spørgsmål vedrørende logningsreglerne: http://www.ft.dk/samling/20121/almdel/reu/bilag/125/1200765.pdf

[1061] http://www.statewatch.org/news/2015/dec/echr-russian-secret-surveillance-prel.pdf

[13] The Court of Justice of the EU judged in the case of Schrems1062 that "legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life". Bulk interception and bulk equipment interference would fall under this category of "access on a generalised basis". The Home Office might argue that ICRs do not constitute content, but they could also arguably come under the same category of overly intrusive generalised access.

[14] That the government has pursued an appeal on DRIPA which may well not be dealt with before the planned enactment of the bill further muddies the waters. Until the CJEU gives its judgement, there can not be said to be a strict and clear legal framework on investigatory powers in the UK, a situation which is of the government's making.

[15] Following Digital Rights Ireland, Schrems and Zakharov the direction of travel is abundantly clear at the European level, both for the ECtHR and CJEU. For the CJEU generalised access is a recurring concern. There can be no doubt whatsoever that the bill as it stands would be subject to legal challenge due to the breadth of its powers.

Definition and workability

[16] As it stands, the definitions in the draft bill lack technical specificity and meaningful clarity. Space precludes listing all the instances, but the most striking examples are the bulk provisions, Internet Connection Records, the intentions regarding encryption and the scope of warrants.

[17] The definitions given for bulk interception in cl 106 (1), bulk acquisition in 122 (5) and bulk equipment interference in 135 (1), merely define these warrants as whether they are issued under a particular chapter with the purposes outlined in that chapter. This gives no clarity on the extent or what "bulk" actually consists of. This means that the public can not possibly take a view on the necessity or proportionality of this legislation. To give a hypothetical topical example, what would actually stop a bulk order defined as "all Muslims"? The current Secretary of State might not take the view that was proportionate, but a future one might have a different opinion. Until "bulk" versus "mass" and "blanket" surveillance can be defined in a way that is meaningful for the public, the question of trust that David Anderson has rightly asked for can not be satisfactorily resolved.

[18] Internet Connection Records are not a recognised industry term. This is a new legal formulation which spells out expected results without specifying how they are to be achieved, how that could be properly costed, and is speculatively predicated on a technology which does not yet exist according to the Telecoms companies.1063

[19] The definition of the scope of subject matter of warrants in cl 13(2) is problematic. In 13(2)(a) "a group of persons who share a common purpose or who carry on, or may carry on, a particular activity" what constitutes a group, a common purpose or a particular activity is

1062 http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf
1063 http://www.theguardian.com/world/2015/dec/15/bt-vodafone-o2-ee-3-cost-feasibility-snoopers-charter

so broad it is difficult to see how the Secretary of State and Judicial Commissioners can make a proper assessment of proportionality. The Intelligence Services Commissioner has already expressed concern over the use of thematic warrants, especially when they are set out in a way which too wide for a proper assessment of the necessity and proportionality.

[20] In cl 13 (2) (b) that "more than one person or organisation, or more than one set of premises" similarly undermines the point of cl 13 (1) in specifying the warrant, and similarly makes assessing proportionality problematic.

[21] The definition in 195 (1) that data "includes any information which is not data" is an obvious paradoxical nonsense.

[22] In the lead up to the announcement of the bill a great deal of focus was given to the question of encryption, and the Home Secretary signalled that the intention was not to "ban" it. However the draft bill leaves a great deal of uncertainty over what could actually be undertaken in relation to encryption and how feasible the approach is. The obligations that may be imposed under cl 189 (4) (c) for relevant operators to remove "electronic protection" apply to anyone providing access to telecommunications, so it must apply to the "over the top" services as well. This would leave encryption as legal, but functionally useless in the UK.

[23] An ability to remove encryption results in vulnerability which may be exploited from any quarter, state or otherwise. The recent "unauthorised" code found by Juniper Networks resulted in US officials investigating concerns backdoor entry allowed tapping of US government communications. It is hard to see how overseas operators would be persuaded to comply in opening up their systems to the potential of such a breach.

[24] Obviously, just having cl 189 doesn't mean that cryptography would disappear. An IP Act could create a situation where average citizens' communication security was weakened, but those who do wish us harm continue to use capabilities out of reach of the legal system. Peer to peer encrypted communications systems exist where it would not really be possible to identify an operator in the sense of the draft bill.

[25] There has rightly been concern that the SIAs and police can continue to function as technology develops. But foremost this is a question of training, recruitment and funding to deal with diversification and change rather than legislation. The temptation will be to leave definitions broad for "future proofing". But this carries the danger of sabotaging rather than proofing the future. For example the "entities" in the Internet of Things and Smart Cities (the government recently supporting the Manchester CityVerve with £10m) will generate an extraordinary new layer of data about people's everyday lives. An application of the powers set out in the bill may seem reasonable now, which may be intolerable just years down the line.

[26] Regarding legality "future proofing", the legislation and its consequences must also be able to withstand a potential "no" vote in the coming EU referendum. A "no" vote will not simply remove the CJEU from the equation. Given Schrems, it is doubtful that a UK with a broad power IP Act in place outside the EU would be seen as ensuring an adequate level of

protection of personal data to allow the transfer of data to or through the UK under EU legislation. This would be catastrophic for the UK tech industry, in particular hosting companies.

Specific Questions
Interception

[27] As laid out in paragraphs 3-6 the case has not been made for bulk interception, nor of its necessity or proportionality as a power.

[28] The only bulk case study given on page 23 of the introduction to the draft bill is not relevant and the case cited in the supporting document on bulk use of s.94 of the Telecommunications Act concern UK **communications data** cases, from previous practices.

[29] Regarding feasibility of Internet interception, section 5.5.2 of the Danish MoJ report details the difficulty with the police system Evident Operator had handling it. Evident Operator was developed primarily to handle telephone interception so practically Internet interception could only occur with specialist IT investigatory support or where the security services were in charge of the investigation. This resulted in a very limited use of logged data, and the law was implemented in a way that section 5.5.1.1 observed was practically useless.

[30] It is welcome that the bill includes an element of judicial approval of warrants. However the provision is still not robust enough for proper oversight and to reassure the public. Warrants should be approved by a judge able to determine on the evidence, not simply review procedure on judicial review principles as in cl 19 (2).

[31] It has been argued, by the ISC amongst others, that the ultimate responsibility for issuing warrants should be with the Secretary of State as they are democratically accountable. This is meaningful only in the most general sense. Practically, because of the secret nature of investigatory powers, there is nothing that citizens can do to hold the Secretary of State to account on individual decisions as they are carried out. This is why the judicial element is important.

[32] Given clauses 17 and 18 on the power of Scottish Ministers to issue warrants it is vital that Scottish opinion is properly consulted, and be seen to be included, on the forming on an Investigatory Powers Act.

[33] The historical issue with the MLATs was set out in paragraph 451 of the ISC report in to the death of Lee Rigby, that US CSPs maintain that providing information to UK authorities would put them in breach of US law. The new arrangements described in the draft bill do not address that fundamental problem, particularly given the broad nature of the powers. There is no clarity as to why the extra-terratorial application of the provisions will be any more successful. Ultimately, this is a question for overseas providers and legal experts, the committee and parliament should seek a range of views from them.

Communications Data

[34] Of all the approaches in investigatory powers law which have failed to keep up with the times it is the concept of communications data. The idea that there are two discrete types of information which are content and communications data, for which accessing communications data is significantly less intrusive is entirely outmoded. Since the advent of mobile devices which connect to the Internet, and social media, those of us who are regular users of Internet enabled devices can have our lives tracked in intimate, even excruciating, detail.

[35] The easiest way to discover what this means for most social media users is to examine the advertising preferences built up for individual Facebook profiles. They list in detail the likes of users covering everything from lifestyle, education, food and drink choices, to sexuality. For most, these listed preferences will both contain the unnervingly accurate and the perplexingly wide of the mark. None of this can be described as '"content" as such. However it does simply demonstrate the dangers of broad access to communications data, as well as relying on filtering to protect citizens.

[36] On a technical level distinguishing between content and communications data as far as web use is concerned is questionable, not least because an Internet connection is most often being used for multiple services simultaneously, with data packets mixed together. Parliament's committees have already heard more detailed information on this matter. Mobile devices continually communicate via apps without the owner making any active decision to do so.

[37] There is no longer any good technical or conceptual reason why communications data as set out in Part 3 and Part 6 chapter 2 should be subject to poorer protections, a different warranty system or a significantly broader access regime. To recognise this does not mean compromising our security or ignoring serious crime. It means concentrating our efforts in a way that is based on how technology has developed. If the committee and/or parliament wish to continue to divide up types of data in a way that is most suited to the postal service, the bill should include provisions for the protection of "enhanced metadata", the combining of different sources of communications data to build up a more detailed intelligence picture. The IPC should have powers to review this and make recommendations.

[38] In neither instance of the case studies on bulk communications data (referred to above in paragraph 28) is it made clear why bulk collection was necessary as opposed to targeted collection.

[39] Section 5.5.2 of the Danish MoJ report shows the issue of feasibility for the police working with significant amounts of communications data. The Danish police used a handling system RAVEN for communications data which took 3 years to come in to use because of problems with the format used. RAVEN was not able to cope with the investigatory and management intentions of the the legislation and the system ended up as just data storage.

Data Retention

[40] The draft bill's proposals are contrary to the principles set out in the CJEU judgement on Digital Rights Ireland and Seitlinger and Others1064. The bill's bulk proposals cover in a generalised manner all means of communication "without any differentiation, limitation or exception" and there are no objective criteria set out for data access. The Court of Appeal took the view that Digital Rights Ireland "was not laying down definitive mandatory requirements in relation to retained communications data" on the appeal of the Davis/Watson judgement1065, but has referred the matter to the CJEU. Even if Digital Rights Ireland is not found to expand the effect of Article 8 ECHR, the reasoning behind the judgement would open up an avenue for a new challenge.

[41] Clause 75 makes clear that CSPs have an obligation to store data effectively, and under clause 182 the Information Commissioner is to be responsible for ensuring this is carried out. What is unclear is if new standards are expected in relation to cl 75, what their specifics would be, how feasible the standards would be in relation to considerable increased burdens on CSPs, and whether the ICO is to be given necessary substantial new resources to carry out obligations under cl 182. At the very least there must be a new funding commitment to the ICO, or the IPC if they are to be responsible.

[42] Despite £650 million spent on "The UK Cyber Security Strategy"1066 by the previous government, its stated 2015 goal that "companies are aware of the threat and use cyberspace in a way that protects … customer data" has far from been universally met. This includes service providers, the most recent high profile example being the Talk Talk breach which resulted in 156,959 customers having personal details accessed, including 15,656 bank account numbers. This was following previous warnings from the ICO to Talk Talk and was the third serious security incident for the company within 12 months. Clearly, the committee will be wise not to take major service providers' assurances on readiness for clause 75 at face value.

[43] A new Information Commissioner is in the process of being appointed. The committee should not report before inviting oral evidence from the new appointee, in particular on the level of resources necessary to carry out obligations under cl 182, whether they consider new sanctions needed for breaches given the greater responsibilities placed on CSPs and if they should have any responsibilities under an IP Act at all.

[44] The cl 75 obligations recognise that poor information security is a threat to the nation and economic well-being. The best way to protect information is not to hold it all if is not needed.

[45] Cl 71 (8)(b) states that requirements may include the generation of data for retention. It is not clear whether this means that companies could be made to generate information that is over and above what is generated in the course of business. The committee should seek clarity on this requirement. This would be a further burden on CSPs, but also change their role from being service providers to being direct investigators.

1064 http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

1065 https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/11/Davis-FINAL.pdf

1066 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

Equipment Interference

[46] As laid out in paragraphs 3-6 the case has not been made for bulk equipment interference, nor of its necessity or proportionality as a power. Even if bulk EI is just to be carried out for the purposes of gathering information, this is the kind of activity that other nation states would characterise as "hacking" or "cyber-attack". There has been no proper debate about the proper security framework for carrying out such activity.

[47] The requirements set out for both targeted interference in clause 93 and bulk interference in clause 140 fall short of the guidelines set out for applications for warrants in 4.6 of the Draft Equipment Interference Code of Practice. Clauses 93 and 140 should also set out as in 4.6 of the DEICP requirements to contain the nature and extent of the proposed interference, details of potential collateral intrusion, what the operation is expected to deliver, details of offences suspected, action necessary to install, modify or remove software. In the case of bulk equipment interference an assessment of potential damage and vulnerabilities that may be incurred should be included.

[50] 7.13 of the DEICP states that the designated official or approving officer must consult the Foreign and Commonwealth Office or Secretary of State in particularly sensitive operations. Any decision to undertake bulk equipment interference overseas is highly sensitive. It should be a requirement to refer any requests to the FCO and the MoD for an assessment of potential security impacts of the undertaking.

[51] It is not generally understood that a class of authorisation for bulk equipment interference can already be obtained for overseas under section 7 of ISA. No specific case example is given in the introduction to the bill. Further supporting material should be set out from the government on the case for bulk equipment interference.

[52] Vulnerabilities constitute a potential threat to national security and economic well-being. It should be a requirement any discovered in the course of equipment interference should be reported to the IPC, who should disclose them to relevant parties, taking security in to consideration.

[53] Part 5 and Part 6 Chapter 1 fail to accommodate the concerns set out on the DEICP by civil society and technology experts in the consultation on the draft code. The committee should revisit this evidence as part of their work.

Bulk Personal Data

[54] Personal datasets can carry extremely sensitive and detailed information about us. Access to personal data is a highly controversial area, and there are very good reasons for restrictions on its use. The Police routinely appeal for help solving crime promising anonymity. A project like Tell MAMA[1067] countering anti-muslim hate crime and measuring incidents would not be able to function properly if victims suspected their information was to be used for other purposes by the SIAs and Police. The storm surrounding the launch of

[1067] http://tellmamauk.org/

Care.data with 700,000 people choosing to opt out of data sharing shows the concerns about the use of health data.

[55] There are no specific limitations on the use of bulk personal datasets, the test of proportionality is not a sufficient protection. The IPC should be able to rule out class BPD warrants and specific BPD warrants on grounds including public health, helping the reporting of crime and protection of victims, and maintaining economic well-being.

[56] The IPC's review remit should also address how BPDs are combined with other investigatory powers, and the proportionality of capabilities that combine them with the results of other powers.

Oversight

[57] The intention to create a unified office under an Investigatory Powers Commissioner is welcome following the recommendations of the 3 intercept powers reports and civil society. It would provide much needed clarity, as it is far from obvious who is responsible for what in the current bodies, or for the wider public that they exist at all. Nevertheless, some oversight functions of the bill are still given to another body, the ICO. For completeness, the obligations under cl 182 should also be carried out by the IPC.

[58] The operation of the intelligence services and police investigations are by necessity covert. The IPC will create a necessary buffer between the public and the SIAs. But the IPC must not become a further protective layer. The new body and its head must be unambiguously the British public's champion. Paragraph 11 of the guide to powers and safeguards in the bill describes the Commissioner as having a role to inform about “the need for” investigatory powers. That should not be the place of the IPC, an advocacy role would place doubt in the public's mind as to the IPC's independence.

[59] Paragraph 11 also mentions a clear mandate to inform Parliament and the public. However, the IPC is appointed by the Prime Minister (cl 167(1)), reports to the Prime Minister (174(1-10)), the PM directs the IPC reviewing of the SIAs (170(1-4)). There should be a public charter for the operation of the IPC with clear goals for investigation of information requests. This charter should contain a plain mission statement of its public remit.

[60] Prompt avowal of capabilities was identified as crucial for public trust by the IRTL David Anderson. Part 8 should include an explicit IPC remit to assess whether new capabilities developed in relation to the powers granted by the bill exceed what is necessary and proportionate in their operation. The IPC should have a duty to report to the Secretary of State or Scottish Ministers to make a recommendation to discontinue a particular practice as overly intrusive, or to avow a particular capability.

[61] Regarding making reports under clause 174, it should be best practice to write them in a way that is as informative as possible, but avoiding the need for redaction under 174 (7). Substantial redaction reduces public confidence.

[62] Given the nature of many of the draft bill's provisions, the IPC should make a detailed qualitative analysis of its functioning to the ISC once it is operational, and a technical report to the Commons Science and Technology Committee.

[63] The right to appeal decisions by the IPT on points of law is a much needed update. The culture of the IPT must also updated to match the IPC with a new emphasis on openness. Part 8 should include that the assumption that hearings are open unless directed otherwise, complainants should be able to appoint special counsel to closed hearings and be informed of such hearings, and detailed reasons given for determinations.

[64] One common complaint is that politicians and civil servants lack fundamental understanding of technological issues. To address this, clause 183 should replace the Technical Advisory Board with the Advisory Council for Digital Technology and Engineering as per the RUSI report's recommendations 4 and 5. ACDTE should also have an ethical use panel.

Summary – Key Points and Recommendations

Overarching / Thematic Questions

A The case made for the broadening of powers has been undermined by the lack of prompt avowal of current capabilities.
B The conclusion from recent security breaches, for example from the Rigby report must be that well supported targeted intelligence should be our national security goal, not bulk powers.
C The Danish experience with session logging legislation demonstrates the problems of necessity, proportionality and feasibility of the proposals in the draft bill.
D The Government has failed to make the case to the tech industry, whose cooperation is needed.
E Roman Zakharov v Russia opens up a route to challenge bulk power provisions in the draft bill.
F CJEU Schrems opens the draft bill to challenge because of the “generalised” nature of bulk powers.
G The draft bill will undoubtedly be subject to legal action if it becomes law in this form.
H The definitions in the draft bill lack technical specificity and meaningful clarity.
I The definitions given for bulk powers in cl 106 (1), 122 (5) and 135 (1) do not communicate what “bulk” consists of in a meaningful way.
J Internet Connection Records are not a recognised industry term.
K The scope of subject matter of warrants in cl 13(2) is too broad to assess proportionality.
L Cl 189 (4) (c) currently means that encryption may not be illegal, but functionally useless.
M The will to “future proof” legislation carries the danger of definitions that are too broad.

Specific Questions

N No case study is given that supports the use of bulk intercept as intended in the bill.
O The judicial element in approving warrants is welcome, but should be strengthened.
P Regarding MLATs, the issue of US CSPs concerns about cooperation breaching US law will be exacerbated by the draft bill provisions, not improved.
Q The assertion that communications data is less intrusive than “content” no longer holds.

R The ability to distinguish between content and communications data is questionable, as an Internet connection is most often being used for multiple services simultaneously.
S There is no longer any good reason why communications data as set out in Part 3 and Part 6 chapter 2 should be subject to poorer protections.
T If communications data is to be distinguished in statute, extra protection should be given to “enhanced” use of communications data, overseen by the IPC.
U The draft bill's proposals are contrary to the principles set out in the CJEU judgement on Digital Rights Ireland.
V The obligations under cl 75 on data protection lack clarity, and it is unclear whether the ICO will be able to enforce them satisfactorily.
W CSPs should not be forced to generate data beyond what they create in course of business.
X Bulk equipment interference should be rejected as an unjustified security risk.
Y The requirements set out for equipment interference should fully incorporate the guidelines set out in 4.6 of the Draft Equipment Interference Code of Practice.
Z Vulnerabilities discovered in the course of EI should be reported to the IPC.
AA If bulk equipment interference is undertaken, FCO and MoD authorisation should be included.
BB The IPC should be able to rule out BPD warrants on specific grounds, including public health.
CC A unified IPC is welcome, for completeness ICO obligations under cl 182 should go to the IPC.
DD There should be a public charter for the IPC, making clear its duties as a public champion.
EE The IPC should have an active statutory role in the prompt avowal of capabilities.
FF The IPC should make a qualitative report on the functioning of a passed IP Act.
GG The right of appeal of IPT decisions is welcome, and IPT accessibility should be improved.
HH The TAB should be replaced by an ACTDE as per RUSI's recommendations.

Acronyms Used

ACTDE	Advisory Council for Digital Technology and Engineering
BPD	Bulk Personal Dataset
CSPs	Communications Service Providers
CJEU	Court of Justice of the European Union
DEICP	Draft Equipment Interference Code of Practice
DRIPA	Data Retention and Investigatory Powers Act
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EI	Equipment interference
FCO	Foreign and Commonwealth Office
ICO	Information Commissioners Office
ICRs	Internet Connection Records
IOC	Intelligence Operations Centre
IPC	Investigatory Powers Commissioner
IRTL	Independent Reviewer of Terrorism Legislation
ISA	Intelligence Services Act
ISC	Intelligence and Security Committee
MLATs	Mutual Legal Assistance Treaties

MoD	Ministry of Defence
MoJ	Ministry of Justice
PET	Politiets Efterretnings Tjeneste (Danish SIA)
RUSI	Royal United Services Institute
SIAs	Security and Intelligence Agencies
TAB	Technical Advisory Board

20 December 2015

Open Rights Group—written evidence (IPB0108)

Who we Are

1. Open Rights Group is the UK's leading digital campaigning organisation, working to protect the rights to privacy and free speech online. With 3,200 members, we are a grassroots organisation with local groups across the UK. Our ethos is that we believe people have the right to control their technology, and oppose the use of technology to control people.
2. Digital technology has transformed the way we live and opened up limitless new ways to communicate, connect, share and learn across the world. But for all the benefits, technological developments have created new threats to our human rights. We raise awareness of these threats and challenge them through public campaigns, legal actions, policy interventions and technical projects.

Summary

3. We welcome the introduction of the draft Bill and the increase in transparency, including the avowing of previously secret activities carried out under implicit general powers. The disclosures of the past two years – triggered by the Snowden leaks – have been astonishing, and have truly transformed our understanding of the Internet and the risks of digital technologies to privacy and democracy. Seeking a "democratic licence to operate", in the words of the RUSI report, should involve a profound debate, and unfortunately this Bill may be too rushed to deliver it.
4. While it is very positive to be able to understand the full spectrum of surveillance powers available to the State, the Bill offers no serious restraint to current capabilities, rather it offers some procedural improvements. Reforms of surveillance in other countries, including the US, are stopping certain practices. In contrast, here some of the most concerning activities – such as bulk acquisition of communications data and thematic warrants – are being brought into the statute book before their very legality has been independently ascertained by human rights judgments in the courts.
5. The debate on those activities should have taken place before loopholes in the law allowed the creation of secret programmes. Parliament has been denied this opportunity, which means many questions have not been debated as a matter of principle, such as whether the data of irrelevant persons ought to be collected and retained.
6. We remain concerned that any areas that are not clearly defined before the Bill is approved – such as Internet Connection Records – may mean that this bypassing of the democratic process could take place again. We would ask the Committee to request absolute clarity from the Government on these and any other issues raised during the scrutiny period.

7. Prior to publication, David Anderson asked that the operational case for further data retention at ISPs for policing needed to be made. An operational case for this has been presented, but this committee has not been given time to fully consider this document. Independent oversight should be tasked with reviewing the operational case. Such a process should be robust and constructed to establish public confidence.
8. The quality of the evidence presented by the Government is lacking in some respects. The presented operational cases for some parts of the Bill needs to be supported with long term data, rather than case studies, in order to assess the actual operational effectiveness of these measures.
9. The operational case for GCHQ's activity should be accompanied by similar supporting evidence. As in the USA, an independent body should be given the task of examining these cases, prior to legislative proposals. Where it has been implemented this has led to the scaling back of programmes mentioned above.
10. The Bill continues to blur the distinction between targeted and bulk surveillance, which is deeply problematic, and aims to consolidate in law the notion that it is fit and proper to spy on the majority of the population in order to target a few.
11. An individual has a right to privacy under Article 8 of the ECHR, which includes a right to be protected by law from surveillance. Legislation permitting the public authorities to have access on a generalised basis to electronic communications compromises the essence of this fundamental right.[1068] Article 10, the right to freedom of expression, is also engaged when the public's right to receive and impart information is impacted. The proposals are chilling –given the bulk and indiscriminate surveillance and lack of limits on time or use – and impact all speech and expression.[1069]
12. We are also concerned that the Bill does not deal properly with the revolution in computer analytics currently underway; big data, machine learning and algorithmic decision-making are transforming many aspects of our lives. The combined use of myriads of bulk data, including Bulk Personal Datasets, in this context will give the State an unprecedented insight into the lives of the whole UK population[1070].
13. Another worrying aspect is the re-appearance of many of the measures included in the rejected draft 2012 Communications Data Bill – popularly known as the Snoopers' Charter. The "filtering arrangements" remain a deep source of concern as they would greatly expand the capacity of the police to perform broad searches across multiple communications providers. Wherever the data is held, the filter would create a queryable database about every individual in the UK.
14. Security risks brought by government hacking remain a major source of concern for digital rights organisations, ISPs and technology companies. Interference with

[1068] See Case C-362/14, Maximillian Schrems v Data Protection Commissioner

[1069] See Liberty and Others v. the United Kingdom, no. 58243/00, ¶56 to 57, 1 July 2008 (the mere existence of a regime for surveillance measures entailed a threat of surveillance for all those to whom the legislation could be applied).

[1070] Keenan, B., 2015. LSE Law Department Briefings on the Investigatory Powers Bill - Bulk Data in the Draft Investigatory Powers Bill: The Challenge of Effective Oversight. *SSRN Electronic Journal*.

encryption and network equipment are particularly worrying, as these can affect large numbers of people.

15. This is a very worrying Bill, with much that is objectionable, despite the improvements in transparency.

Interception

Targeted Interception

16. Targeted interception of communications under strict conditions has a place in a democratic society, but we are concerned about some of the new powers introduced in the statute book by the draft Bill.
17. The main source of concern is the creation of "thematic warrants" under Cl.13(2), allowing the targeting of "a group of persons who share a common purpose or who carry on, or may carry on, a particularly activity", without the need for such individuals to be named, or even known. This power would appear to be equivalent to the general warrants outlawed hundreds of years ago,[1071] and we believe should be removed from the Bill.
18. We would also urge caution about the powers in Cl.12(8) to extract data from content, presumably email addresses or calendar events. Treating such content as data would enable the automated analysis of such materials, and the implications should be explained in more detail.
19. Text and data mining for patterns and other insights unrelated to the meaning of an individual message is important in many areas, including security, but this should be closely supervised. For example, German academic Andrej Holm was mistakenly arrested in 2007 after a computer found linguistic similarities between his writings and the communiqués of a radical group.[1072]
20. The provisions for the modification of warrants in Cl.26 should be tightened. The Secretary of State and senior officials would have very broad powers to change names, premises, or even to add multiple names without requirement for judicial commissioner approval. Such major modifications to a warrant would appear to deserve a similar level of scrutiny as the original authorisations.

Bulk Interception

21. We have read carefully the arguments from the three major reviews of surveillance in support of bulk interception, and remain unconvinced that the case has been sufficiently made as to its on-going effectiveness in relation to its level of intrusion.
22. The bulk interception of communications, as described in the GCHQ documents released by Edward Snowden, has no place in a democratic society. Bulk interception is meant to be directed overseas, but as Government lawyers have admitted, this

[1071] http://www.parliament.uk/about/living-heritage/evolutionofparliament/houseofcommons/reformacts/overview/wilkeslib1/
[1072] https://www.eff.org/node/81889

activity involves collecting wholesale communications of a large majority of people in the UK, including MPs.[1073]

23. The Internet is by its very nature global and the distinction between domestic and overseas communications provided in the Bill is unworkable. In practice all traffic flowing through tapped cables is copied, broken down, analysed and classified – webmail, emails, chat, Internet browsing, website logins, webcams, gaming, social networking – with billions of records stored for up to six months.[1074]
24. The safeguards proposed are not enough. Such indiscriminate collection, storage and analysis go against the direction of various rulings by the European Court of Human Rights, and we cannot see how it is legally sustainable.[1075]
25. Only a small amount of collected information relates to suspects, in the UK or overseas, but GCHQ has made the case repeatedly that they need to hoover up everything. A much more targeted form of Internet surveillance – based on concrete suspicion – should not be beyond the reach of our well-funded intelligence agencies. Extraction of only targeted materials from the traffic is technically possible if the aim is to find known suspects, rather than generating new insights at the population level.
26. Strict requirements for the minimisation of data collected and stored at every level should be written into the Bill. Some such requirements can be found in legislation elsewhere. US bulk surveillance systems have to comply with United States Signals Intelligence Directive 18 (USSID-18) on "Legal Compliance and U.S. Persons Minimization Procedures" setting out constitutional compliance during SIGINT operations. USSID18 was put in place in 1980 as part of the tightening of the US surveillance regime following the Watergate scandal.
27. USSID 18 sets fairly detailed criteria for how information can be collected, processed, retained and disseminated. For example, it sets out that communications between persons in the US accidentally collected in foreign surveillance must be promptly destroyed (section 5.4.b) unless they are specifically relevant.
28. While we would not consider that this is enough to make "bulk surveillance" legitimate, it shows that it is possible to place restrictions on data handling which however are not present within the proposed UK legislation.
29. Oversight bodies need to be able to interrogate in detail the actual practices of agencies in order to provide a clear line of accountability from technical implementation and authorisation all the way to possible challenges at human rights courts.

[1073] http://www.theguardian.com/uk-news/2015/jul/24/wilson-doctrine-unworkable-bulk-interception-intelligence-agencies

[1074] GCHQ, Data Stored in BLACK HOLE - The Intercept. Available at: http://theintercept.com/document/2015/09/25/data-stored-black-hole/ [Accessed September 25, 2015].

[1075] See Chapter 7 of our report on mass surveillance available at https://www.openrightsgroup.org/assets/epub/Collect_it_all.epub

Content and metadata

30. The focus on content in Cl.119(4)b is misplaced. Data is analysed in bulk without any extra warrants, and only at the end of the process will a targeted examination warrant be sought, only for some types of data and if the target is in the UK. Collaterally collected data is much more important than content for Internet surveillance as it uniquely allows for the mapping of behavioural patterns and social relationships.
31. The general distinction between content and metadata (Cl.193) and the reduced protection for the latter is flawed. Metadata may allow "*very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained"* and the retention of metadata relating to a person's private life and communications is, in itself, an interference with the right to privacy.[1076] There is a lack of specificity in the Bill about what constitutes metadata and therefore receives no protection. This should be precisely defined, in particular, in relation to live and historical location data.

Bulk Communications data

32. The previously secret regime for the acquisition of bulk communications data under the Telecommunications Act 1984 has only been admitted with the publication of the draft bill, which will replace the former provisions, bringing them clearly into view in the statute.
33. The Government created an access regime for communications data, with special authorisations and procedures sanctioned by Parliament under RIPA. We now learn that successive Secretaries of State bypassed Parliament, abusing legal loopholes to create a secret bulk access mechanism without regard to the Home Office's own statutory Code of Practice on the Acquisition of Communications Data. These activities had no known oversight until 2015. These revelations are extraordinary and deserve an inquiry of their own.
34. The published *Factsheet on Bulk Communications Data* summarising how services currently implement this power describes data-mining practices that can identify "patterns of activity" and "the links between individuals or groups". The Bill would introduce some procedures and safeguards, but ultimately the main effect would be legalising the mass surveillance of the UK population.
35. The Factsheet stresses that bulk communications data could only be obtained "in the interests national security"; but as the Handling Arrangements also make clear, under Section 19(2) of the Counter-Terrorism Act 2008, *"information obtained by any of the intelligence services in connection with the exercise of any of its functions may be used by that service in connection with the exercise of any of its other functions."* For

[1076] See cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others* and *Copland v the United Kingdom,* No 62617/00 ¶¶ 43-44; cf. *Rotaru v Romania*, No 28341/95, Judgment (GC) ¶ 46 (same)

example, information obtained by MI5 for national security could be used to support police investigating serious crime.

36. In addition, the new regime would expand existing bulk acquisition. The Handling Arrangements for bulk data obtained in the current regime – published with the bill – exclude ICRs, but there is nothing in the draft bill carrying through these restrictions after the current provisions are superseded by the IPB. This may allow the Security and Intelligence Agencies to perform sophisticated analytics able to generate new leads on potentially suspicious behavioural patterns, but it would mean analysing the Internet usage of the UK population. This is even more intrusive than mapping relationships among phone calls.
37. Similar measures for bulk access to phone records in the US under section 215 of the Patriot Act have been stopped. In January 2014, President Obama announced the end of the NSA bulk telephony metadata program. Instead, the President indicated that the data should remain at the telephone companies, with targeted individual orders from the Foreign Intelligence Surveillance Court (FISC) using narrow selector terms (name, numbers, etc). In June 2015, the USA FREEDOM Act confirmed this in law and from November 2015 the bulk metadata collection programme has officially ended. The US regime does not contain extra retention measures and relies on data normally kept by companies for their own business purposes.
38. We do not believe that admitting the existence of these provisions for bulk access and adding some controls will make them proportionate, and this whole part of the Bill should be scrapped and replaced by targeted requests. There is no doubt in our mind that this part of the Bill will be subjected to – likely successful – legal challenges.

Bulk Personal Datasets

The Committee asks: Is the use of bulk personal datasets by the security and intelligence services appropriate? Are the safeguards sufficient for the retention and access of potentially highly sensitive data?

39. The provision in Part 7 of the Bill for the acquisition of "Bulk Personal Datasets" (BPDs) is disproportionate. Understandably, the security and intelligence services should be able access a variety of databases in their investigations of crimes and people who are suspected of criminal activity. However, getting hold of all the information in multiple databases to perform undetermined processing is mass surveillance. The definition of BPDs in the Bill and the growing prevalence of datasets mean the measure is likely to affect the entire population, the majority of whom are innocent of any crimes.
40. The fact that this is already happening and authorised elsewhere - with the Bill merely bringing their handling processes into the statute book - does not make this power any less excessive. The "double-lock" provisions, similar to those found elsewhere in the Bill, would not be enough to ensure that this kind of surveillance is

necessary and proportionate. The intrusiveness of databases can grow exponentially when combined with other data sources. It is hard to see how the commissioners – or indeed the committee – might be able to make a proper judgement without a deep understanding of the full database estate held by the agencies and the state of the art computer analytics available.

41. The case for bulk processing has not been thoroughly made, only a factsheet has been presented, which falls far short of the necessary process of presenting a case for thorough independent examination There is no consideration of alternative forms of access to individual records, nor any distinction between gateways to government databases and accessing those of the private sector, possibly by covert means. The potential scope of these databases is unlimited, without clear policy criteria to guide acquisition and usage.
42. The Bill does not create a new power to compel any organisation to provide data, but leaves the door open for the agencies to obtain any and all databases containing personal information, making it very difficult to see where surveillance ends in this regime. This is taking place in the context of a huge expansion in the number and richness of databases available in both the public and private sectors.
43. In addition there are a number of issues with the formulation of the power in the Bill. BPD warrants can be issued for *classes* of data – such as travel – without specifying exact databases. This seems far too broad, and if anything at the very least there should be maximum transparency over what datasets can be accessed.
44. The Impact Assessment for BPDs raises concerns that criminals would be helped to escape detection by increased transparency, changing their behaviour if they knew about the databases held by the intelligence agencies. While in some very specific cases this may be true, the examples of bulk datasets circulated – firearms, travel, DVLA – are very large and appear to pose little risk of pinpointing at specific investigations.
45. The Bill contains provisions that would appear to enable the intelligence services to routinely obtain databases and carry out initial examinations in order to determine their usefulness without any warrant[2]. The Bill would also allow the agencies to retain data without a valid warrant[3] under the discretion of the Judicial Commissioners.
46. The current guidelines for the handling of BPDs contain some troubling indication that low level officials are obtaining data without consulting senior staff:
47. “4.5 These can be difficult and finely balanced questions of judgement. In difficult cases staff should consult line or senior management and/or legal advisers for guidance, and may seek guidance or a decision from the relevant Secretary of State.”
48. There are particular concerns about sensitive data, such as medical records, and the provisions in the accompanying handling guidelines are too vague. The Bill should restrict access to data recognised as sensitive in data protection legislation.

Internet Connection Records

49. We see Internet Connection Records (ICRs) as one of the most problematic aspects of the Bill. Unlike other areas, they are an apparently new form of data acquisition posing new risks of excessive collection, as well as more prosaic problems such as cost.
50. As they are not properly defined and introduce excessive uncertainty, we have doubts as to whether they are workable at all, and consider that their intrusiveness has been grossly underestimated.
51. We believe that the proposed ICRs will by necessity require performing very sophisticated analysis of Internet traffic. In order to dig deeper into users' activities, including the use of messenger applications such as Skype, ISPs would need to monitor flows of data, reconstructing individual activities, to then generate an associated log of "Internet connections".
52. ISPs giving evidence to the Committee have raised serious concerns about the associated costs and we have been given similar indications by many technology experts.
53. This level of monitoring and detailed analysis is more akin to interception and reporting than retention of data,[1077] and this is a fundamental flaw in the proposals.

Retention

54. The Operational Case for the Retention of ICRs presents ICRs in very limited terms:
55. ICRs comprise a very narrow set of data, such as numerical internet protocol (IP) addresses and port numbers – which may be used to establish that a particular device accessed a particular internet service or website – as well as details of the time that a specific service was accessed.
56. Unfortunately, this concise definition is not reflected in the actual bill. ICRs are not properly defined in Clause 71(9) of the Bill which provides for the retention of "relevant communications data". The retention regime is broader than in the current Data Retention Regulations 2014[1078] and the creation of ICRs could involve many types of data.
57. ICRs are only defined in the actual Bill by their use and access regime,[1079] and could be understood very narrowly as described in the Operational Case, or quite broadly as involving any types of communications data required to identify Internet connections. The requirement to **create** and retain this kind of data is completely new. As many Internet Service Providers have told the Joint Committee, ICRs are not something that exist or are kept. They would need to be generated.

[1077] http://www.projectpact.eu/privacy-security-research-paper-series/%231_Privacy_and_Security_Research_Paper_Series.pdf
[1078] http://www.legislation.gov.uk/uksi/2014/2042/schedule/made
[1079] Cl.47(6)

Access

58. The documents supporting the draft bill stress that there would be strict limits on access to ICRs[1080], but we see several problems with the proposed access regime.
59. ICRs will be accessed under the general regime for communications data, which means that there would be no judicial authorisation or "double lock" for accessing Internet Connection Records. Only if there is a review of the retention notice, on referral by a telecommunication operator, does the Secretary of State need to consult the Investigatory Power Commissioner (IPC), although he or she is not obliged to accept any recommendation of the IPC (Cl.73).
60. This ignores the lessons from the Digital Rights Ireland case, where the Grand Chamber noted that "above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions."
61. We are also concerned that the above access provisions do not restrict what can be done with new types of Internet data that would be retained in order to generate ICRs. Additional safeguards would be needed to ensure that the underlying data is not be accessed for other purposes.
62. The use cases presented to justify retaining ICRs are based on police work and individual access, but the records would likely be subject to the bulk acquisition powers and the "filtering arrangements".

Use

63. Clause 47 (4) of the draft Bill restricts the purposes for obtaining ICRs (or derived data). The purposes of identifying the sender of a suspicious communication or those accessing illegal materials are fundamentally different from knowing everything a person does online.
64. In investigations on known suspects ICRs would appear as an alternative to problems that could be solved by other less intrusive means. Security services have access to the full Internet history of suspects in criminal investigations through the use of targeted intercept warrants. The preferred solution here would be to make interception available for a wider but specified range of purposes – including missing children –, and admissible in court as is the case in most democratic countries.
65. The police should be efficient and effective and not suffer excessive burdens. But the operational case for ICRs does not discuss the relative proportionality of different forms of intrusion, just how technology could help minimise police efforts. A more

[1080] Guide to powers and safeguards p. 26

balanced analysis is needed. Technology opens up possibilities for what can be done, but this does not mean it should be done.

Intrusiveness

66. Cumulative information of websites visited can give a good picture of someone's lifestyle, political views and personal issues. Single visits to some sites can be sensitive even if we only know, for example, that someone visited an abortion clinic's site but not the specific sections of that site.
67. In addition to the risks to individual privacy there are wider issues of democracy. The Bill would create a distributed database of every website visited and mobile app used by every person in the country. The ability to process this pool of data through bulk acquisition in order to build an understanding of sustained patterns of behaviour at the population level is highly intrusive.

Security

68. We consider that the proposals do not sufficiently consider the security risks of generating and storing this kind of information. We have seen many data breaches in recent times. The attacks on ISP TalkTalk showed that poor security is widespread even among major companies.[1081] Despite clauses in the bill requiring security measures, nobody can promise the data will be 100% safe.
69. ISPs may hold the data separately or perhaps in a single joint centralised database. Once collected together and made interrogable via the "filter" the data becomes an extremely intrusive engine for population level analytics, and any apparent physical separation of data becomes irrelevant. We examine this in the section about the filter, but we should regard the two proposals as essentially part of the same national "communications database" proposal.

Lack of definition

70. Despite the various documents and explanations accompanying the draft bill, there is a lack of clarity as to what exactly will constitute an ICR. Operators would be forced to record logs of access to online services, but there could be huge differences on how this is interpreted and the impact of the measures.

Extended scope

71. The discussions on ICRs are mainly circumscribed to Internet Service Providers. Once data retention provisions are extended to other Internet companies such as providers of Virtual Private Networks it will be increasingly difficult to precisely define what may be an ICR.
72. ORG believes that the measures to introduce ICRs are problematic and should be removed from the current legislation until these issues are clarified. David Anderson

[1081] http://www.theguardian.com/technology/2015/oct/23/talktalk-criticised-for-poor-security-and-handling-of-hack-attack

did not just ask for an operational case for ICRs. His full recommendation should be satisfied before ICRs are introduced in the statute book:

73. "There should be no question of progressing proposals for the compulsory retention of third party data before such time as a compelling operational case may have been made, there has been full consultation with CSPs and the various legal and technical issues have been fully bottomed out. None of those conditions is currently satisfied."

CJEU ruling, April 2014

74. The 2006 Data Retention Directive (Directive 2006/24/EC) which required communications service providers to retain customer data for up to two years for the purpose of preventing and detecting serious crime, breached the rights to privacy and data protection under Articles 7 and 8 respectively of the EU Charter of Fundamental Rights. The Grand Chamber observed that the scope of the data retention "entails an interference with the fundamental rights of practically the entire European population" (¶56).
75. The Court went on to note the Directive was flawed for not requiring any relationship between the data whose retention was provided for and a threat to public security (¶59). The Grand Chamber found it amounted to a "wide-ranging and particularly serious interference" with the rights to privacy and data protection "without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary". (See C-293/12, *Digital Rights Ireland v Minister for Communications and others.)*
76. The mandatory data retention regime under the Bill will go much further than what was prescribed under the Directive—in so far as it will not only be limited to the detection or prevention of serious crimes, but for any of the grounds under which communication data can be requested (§46.7) and, it seems, for any other purposes whatsoever (§5(2) and (3)). While the Judicial Commissioner is to check proportionality in appeals, no prior or subsequent judicial authorisation is required for retention orders.

Filtering Arrangements

77. One of the most concerning aspects of the draft bill is the "request filter", previously proposed as part of the rejected Communications Data Bill. The filter would allow the police and authorised public bodies to analyse retained communications data, as preparatory work before applying for individual warrants targeting specific data.

78. The exact architecture of the filter is not clear. From the oral evidence given to the Committee by ISPs, based on conversations with the Home Office, it seems that a 'third party" would receive communications data in bulk1 and operate a search engine that would allow the police to query the data.
79. The picture that emerges is that the filter may be only one component of a single surveillance system that relies on various powers in the draft bill. The provisions for

the acquisition of bulk communications data could be used to build a central repository accessible to the Security Service for large-scale data mining. The filter would then create a more limited gateway for ordinary police to perform more limited searches over this data.

80. We believe that the public should be clearly informed of the implications of what is being proposed and the Bill and accompanying documents are not transparent enough. The filter would be best described as a single government controlled database that would be maintained at a central location on behalf of the Home Office. However, this "filter" is described in the impact assessment purely as a *safeguard* because it would potentially reduce the amount of data that would be eventually forwarded to the police.
81. We are concerned that despite assurances against fishing expeditions, the filter-database could be used for the discovery of completely new surveillance targets by combining searches across data types and company repositories. For example, with only an internal authorisation police would be able to easily identify all participants at multiple political demonstrations broadcasting critical videos from their mobile phones. By conducting intrusive data mining across a range of data sources, the "filter" violates the privacy of an unlimited number of innocent people.
82. Such a tool could be expanded as new secret data retention orders may cover new forms of data transmitted over communications networks, such as smart meters, leading to mission creep. The intrusiveness of storing details of all online activities of the population grows exponentially with the "filter".
83. In addition there are many unanswered questions about the security of such a database and who would be responsible for breaches. At present it is unclear whether a "third party" would be a private contractor or government organisations, such as the National Technical Assistance Centre (NTAC). The security risks would apply to all citizens whose data had been retained. This could be a heavy price for people to pay for the alleged policing benefits.
84. This filter and database would affect almost every citizen, in that their data would be available for analysis and the limited safeguards and access controls are not enough to guarantee it could not be abused. Even with better safeguards, the prospect that data can be analysed, retrieved and misused would be disproportionately chilling for political and journalistic activity.

Other Issues

85. The Bill touches on many other issues that we believe are extremely important but we have been unable to cover in detail. Given the timescale we have focused on the areas most relevant to our organisation but here we list some other issues we believe need to be examined by the Committee.

86. In some case these issues will have been covered more extensively in submissions by other organisations such as our partners in the Don't Spy on Us coalition (Article 19, Big Brother Watch, English PEN, Liberty and Privacy International).

Encryption and technical capabilities

87. There is widespread concern in the technology sector that Cl.189 could be interpreted as imposing such a requirement on providers to remove encryption to support aspects of the Bill. The Home Secretary has stressed that there are no new powers on encryption in the Bill. If Government does not wish to impose these measures this should be explicit and clear on the face of the Bill. Otherwise, these capabilities should be regulated much more thoroughly.

Equipment Interference / Hacking

88. This is a critical area that has only recently been properly acknowledged, despite its importance. We would endorse the submission of our colleagues at Privacy International in this area.
89. We are particularly concerned about the breadth of these powers to affect large groups of people, (not just in bulk hacking), and how innocent third parties may be targeted as collateral. The implications for wider Internet security are unclear and the agencies should be liable for any clean up of damages. The co-option of third parties such as communications providers to assist in the interference (Cl.101, 145(4)) is particularly worrying.
90. The intrusion involved in hacking and the risk to security of communications raise such serious human rights concerns that a high standard of scrutiny and proper judicial authorisation must be required. Instead, Part 5, the supposedly "targeted" hacking provision, permits attacks on broad categories of equipment that could include that belonging to communications service providers. Part 6, Chapter 3 of the Bill compounds this problem by allowing hacking to be carried out "in bulk" when it is directed overseas.
91. This "bulk" provision gives unfettered powers to the intelligence services to decide who and when to hack. There was already very wide discretion under earlier and more detailed processes stipulated in RIPA and we cannot conceive how this new approach is consistent with recent law.[1082]
92. There is evidence that ordinary activists, NGOs and human rights' defenders have been targeted by state-sponsored equipment interference attacks worldwide.[1083] Often their work is very clearly in the public interest and yet the Bill does not outline any meaningful measures likely to provide any safeguards or protections for these

[1082] see *Kennedy v. UK,* 26839/05, and *Zakharov v. Russia* 2015 (47143/06)

[1083] http://www.theguardian.com/world/2010/jan/14/china-human-rights-activists-cyber-attack
http://arstechnica.com/tech-policy/2015/12/beware-of-state-sponsored-hackers-twitter-warns-dozens-of-users/
https://googleonlinesecurity.blogspot.co.uk/2012/06/security-warnings-for-suspected-state.html

groups – despite the public interest in the debates they engender and their crucial role in democratic societies.

93. Based on the evidence to the Joint Committee on 16 December 2015, there is a significant gap in public knowledge about how equipment interference powers are being used and their frequency and we need much greater information in the public domain and to encourage and inform and not curtail public debate.

Judicial authorisation and oversight

94. We echo the concerns of Liberty and others civil society groups about the supposed "double lock", including the limitations of judicial review. The independence of judges is a key consideration to make surveillance legitimate. In *Zakharov v. Russia* 2015 (47143/06) [GC], although the Russian system required prior judicial authorisation (¶259] it was not considered sufficiently independent nor able to counter the breadth of the state powers. The proposed Judicial Commissioners lack full independence and are somewhat captured by being appointed via the executive. Only the ordinary courts can provide the independence necessary –via ordinary serving and rotating judges sitting in the higher courts. Rulings must be public and hearings adversarial—with adequate protections when needed. It should be recognised that individualised prior judicial authorisation in itself will not always restrain mass surveillance systems.
95. When authorisation is required in the Bill, these 'Judicial Commissioners' are only required to apply the "same principles as would be applied by a court on an application for civil judicial review" – namely *Wednesbury* unreasonableness or irrationality and not the Warrant Standard appropriate in a criminal context.[1084] This approach will limit the review to procedural aspects, as it has in the past.
96. These limitations are exacerbated in the case of "bulk" warrants, where authorisation requests could be formulated in such broad ways to make assessments on the merits of the applications challenging. Further, necessity and proportionality assessments need only take into account "whether the information which it is considered necessary to obtain under the warrant could reasonably be obtained by other means",[1085] and not the appropriate standard of whether other less invasive techniques have been exhausted or would be futile, so that the techniques used is the least invasive option.
97. The proposed system also reduces appropriate neutral and detached judicial oversight due to the lack of separation between the authorisation and oversight functions of the Commissioner's office. Similar arrangements by public prosecutors in Russia were recently criticised by European Court of Human Rights in the Zakharov v Russia case for raising doubts about independence (§280).

[1084] Cl.19.2, 109.2, 123.2, 138.2, 155.2
[1085] Cl.14.6, 107.5, 122.4 and 137.4

98. Our additional concern is that the Bill leaves untouched the authorisation regime for communications data, which continues to be a purely internal affair despite the improvements around Single Points of Contact. Human rights courts have been consistent on the need for independent authorisation at every level.

Transparency

99. The Government has avowed many secret powers with this BIll, but the authorisation and oversight system will continue to be a closed box that maintains surveillance fully within the circle of secrecy. The Bill is too short a step to bring surveillance into the 21st century world of open government that drives transformation elsewhere.

100. The Bill also expands the secrecy regime around surveillance measures, including various offences of unauthorised disclosure.[1086] The offences in the Bill must provide express public interest defences in order to protect whistle-blowers and investigative journalists as well as to increase public trust. Without such amendments, the new offences in the Bill will have the effect of widening rather than narrowing that gap to make CSP employees and contractors subject to Official Secrets Act-type restrictions and penalties.

101. Protections should also extend to security researchers working in the public interest to avoid ambiguity around the practices of computer security research, whereby freelance computer security experts search for, analyse and report on vulnerabilities in the systems of technology firms, sometimes in response to incentives from prominent technology companies, as an integral part of troubleshooting and perfecting network security. Researchers working in this field already face legal uncertainty. The wording in the present bill potentially criminalises this important work.

102. The “tipping off” of criminals should be certainly tackled, but given the broad non-targeted dimension of much of the Bill, these provisions could be tightened to enable ISPs to discuss best practice and more transparency over general capabilities affecting the majority of the population.

103. For bulk orders, "tipping off" is not a concern as such orders will affect a large number of individuals (not suspected of any wrongdoing whatsoever) so a permanent prohibition on revealing anything about these orders, which are matter of intense public concern and directly and seriously impact fundamental rights, is unnecessary and disproportionate and likely to inhibit important public debate in the public interest.

104. The ISC called for greater openness. Concerning targeted warrants, the ISC recommended that, contrary to the blanket prohibition under RIPA, "*disclosure [of a specific interception warrant] should be permissible where the Secretary of State considers this could be done without damage to national security.*" We consider §66 in particular, would be better framed as a general expectation that orders for

[1086] Cl.44, 66, 102, 133, 148, 190

communications data will become public at some point in the future, subject to an official veto where it is operationally necessary.

105. The three provisions relating to targeted warrants, and the criminalisation of notifying the subject of a notice – indeed notifying "anyone;" may inadvertently prevent communications service providers from releasing aggregated, anonymised information about the official requests they receive. In recent years, an increasing number of communications service providers have started releasing transparency reports, which have done a great deal to improve public understanding.

106. Indeed, in the aftermath of the NSA scandal, a number of CSPs in the US reached an agreement with the US Government, allowing data on official orders to be disclosed in a set format. Enabling CSPs to release this kind of comparative data would provide an important complement to the information currently issued by IOCCA. Nothing should prevent CSPs producing their own Transparency Reports. Where such international, anonymised and aggregated data is available, this provides an important complement to the information currently issued by UK authorities.

107. Section 77 imposes a duty for "a telecommunications operator, or any person employed for the purposes of the business of a telecommunications operator" not to disclose the existence or content of a data retention notice. While the duty to comply with a data retention notice is not new, the duty to keep secret the "contents" of such a notice is. The Bill is considerably more opaque in this respect than previous data retention legislation, not least due to the ambiguity as to what constitutes an "Internet Connection Record". A strong case needs to be made for imposing secrecy where information was formerly available, particularly as this impacts the Articles 8,9 and 10 rights of all who use a UK ISP.

Notification

108. The Bill introduces a welcome but insufficient power for the IPC to inform an affected person of serious errors that have caused prejudice (Cl.171), and a right to apply to the IPT for details. The system would rely on the judgement of the IPC as to the seriousness, and there is a real possibility that the error in question would involve the Commissioners Office's authorisation functions.

109. The lack of provisions on notification and the strict prohibitions for unauthorised disclosure, deny individuals the knowledge and ability to seek redress for unlawful surveillance. A monitoring scheme will not be 'in accordance with the law' if it fails to ensure that persons who are monitored are notified of the surveillance (if only ex post facto).[1087]

110. We believe that individuals who are subject to surveillance should be legally notified when there is no risk of jeopardising an on-going investigation or there is an imminent risk of danger to human life. This should ordinarily happen within 12

[1087] See *Assn. for European Integration and Human Rights & Ekimdzhiev v Bulgaria*, 62540/00, a t ¶ 90-91.

months of the conclusion of the investigation, although that 12-month period may be extended by a judicial authority in six-month intervals. An express duty of full disclosure and good faith should be imposed on the services seeking to delay notification. Consideration must be given to how citizens are able to seek redress if they have no means to find out if they have been subjected to surveillance.

111. Surveillance data must be made available to criminal defendants and the prohibition on this removed (§42). This is another crucial check and balance but also the point at which violations of law impact the rights of the individual and their Article 6 rights most significantly.

Foreign collaboration and PRISM

112. The Snowden leaks revealed the extent of collaboration and information sharing among intelligence agencies, particularly the NSA, despite the severe limitations in place for collaboration among police forces. These activities are not properly regulated and the Bill does not tackle this matter.

113. There are some guidelines on the passing of information overseas (Cl.41, 118) and for requesting data under mutual assistance. Foreigners must have the same protections as UK citizens to protect all citizens from unfettered sharing of data gathered by co-operating governments. We note the data may again be transferred overseas "*to the extent (if any) as the Secretary of State consider appropriate*" (Cl.118.2). A transparent and rule based mutual sharing framework must be provided for with reciprocal protections and standards required – as in the civil law data protection regime. There should also be prior judicial oversight before any transfers and the Warrant Standard should be adapted.

114. There is however a concerning provision for the interception at the request of a foreign power (Cl.39) with no apparent supervision or signoff by ministers or judges. The explanatory notes suggest this would only cover individuals outside the UK, but such restriction is not in the Bill.

115. The Bill does not appear to address one of the main issues raised by the Snowden leaks: the receiving of content and data from overseas, including the NSA's PRISM programme. The Intelligence and Security Committee stated, after an investigation,[1088] that GCHQ did not circumvent any laws when accessing content via PRISM. General access is authorised under the Intelligence Services Act 1994, and when GCHQ sought information from the US, a warrant was in already in place under the RIPA. This is stretching the regulatory regime.

116. Since the initial revelations about PRISM, we have learnt that GCHQ had direct access to PRISM during the 2012 London Olympics, with 100 operatives generating some 11,500 extracts in a six day period.[1089] More recently GCHQ have

1088 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/225459/ISC-Statement-on-GCHQ.pdf

1089 https://firstlook.org/theintercept/article/2014/04/30/gchq-prism-nsa-fisa-unsupervised-access-snowden/

requested a permanent arrangement for full and unsupervised access to PRISM, although it is not known whether this request has been approved by the NSA. The Bill should explicitly regulate this kind of foreign collaboration and put adequate safeguards in place.

Definitions

117. The Bill subtly expands the surveillance regime through the modification of established definitions that determine the scope of the powers defined elsewhere in the Bill.

118. Clause 193 (10) defines "telecommunications operator" in a way that can be interpreted very broadly. The example given in the Home Office's documentation is an Internet Service Provider (ISP) but we believe this definition could include many other organisations who provide an Internet network of sorts. As much of the Bill would now cover private networks, all kinds of access and connection logs could be demanded from many UK organisations. In some cases it may be difficult to establish who exactly is the operator, such as in subcontracted or collective Internet provision in hospitals or schools.

119. The definition of "apparatus" in Cl.195(1) now includes "whether physical or logical", leading to concerns that this could be interpreted to cover suppliers of software, who could be asked to implement capabilities.

120. The new definitions of *event data* and *entity data* may cut across established categories of traffic and subscriber data and should be tested for consistency with other legislation such as e-privacy. The Bill assumes that entity data is less intrusive than events, but social graphs would be included, and these are highly intrusive. The scope is hugely extended beyond the more restrictive *traffic data* in current legislation.

Bypassing appropriate channels to obtain communications data

121. The provisions in Cl.46(4) would allow an authorised officer to ask any person not in possession of the communications data but *capable of obtaining* it to obtain it and disclose it. This could be read from going directly to the company's IT department to asking external *hackers.* It is known that GCHQ has a program to develop HUMINT, which involves running covert agents in the telecommunications industry,[1090] who could be asked to provide data bypassing official channels.

General authorisation for the use of information

122. Section 19 of the Counter-terrorism Act 2008 states that information obtained by any of the Intelligence Services in connection with the exercise of any of its functions may be used by that Service in connection with the exercise of any of its

[1090] Greenwald, G., Ball, J. & Borger, J., Revealed: how US and UK spy agencies defeat Internet privacy and security. *The Guardian*. Available at: http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security [Accessed September 05, 2013].

other functions. For example, information that is obtained by the Security Service for national security purposes can subsequently be used by the Security Service to support the activities of the police in the prevention and detection of serious crime.

123. The implications of this principle for the application of any restrictions on purposes introduced throughout the Bill should be clearly explained.

Expanded ability for ISPs to intercept traffic

124. Clause 33 expands the lawful capacity of telecommunications service providers to intercept communications for their own purposes, including website blocking, Internet filtering; spam, security and so on.

125. This is problematic on two accounts. Interception, even by communications providers, should be limited to encourage freedom of expression, and importantly any such interception will likely generate logs that can be added to data retention orders, fuelling further surveillance.

National security notices

126. Clauses 188-190-1 give the Secretary of State the power to order any telecommunications operator in the United Kingdom to take such specified steps as the Secretary of State considers necessary in the interests of national security.

127. These notices cannot cover any aspect covered by warrants in the Bill. Experience shows that such general powers as those in the Telecommunication Act 1984 may enable new surveillance practices without scrutiny and should be severely limited.

Sources and Privilege

128. The Bill offers wholly inadequate protection for journalists and their sources (§61)—a serious threat to the vital press function as a watchdog of democracy. For the press to operate as a watchdog of democracy, it needs sources. It is difficult to see how this can be reconciled in a meaningful way with the bulk acquisition and processing regimes in Part 6 of the Bill. The safeguards for journalists extend only to police and not intelligence services. Journalists should not be prosecuted for receiving, processing or publishing classified information in the public interest and must also be properly protected from the offences (see further below). There should also be more clarity about how legal privilege will be maintained.

21 December 2015

William Perrin—written evidence (IPB0156)

Is a copy of the ANPR database held by the agencies, should it be avowed as a Bulk Personal Data Set, what is it used for and what the data retention policies?

I am a member of the former Crime and Justice Sector Transparency Panel – a recently abolished body that used to help Ministry of Justice, the Home Office, the police etc with transparency issues. My findings on the nature of the Automatic Number Plate Recognition system run by the police forces may be of interest to the committee.

ANPR is a colossal surveillance system, each year recording billions (billions) of 'reads' of peoples number plates. It is possibly the world's biggest civilian-run surveillance system. I strongly support ANPR's operation but have criticisms of its governance and data retention policies. ANPR is an activity carried out by the police underpinned by the Data Protection Act. Through FOI requests I ascertained that the Metropolitan Police has held since 2012 an aggregate copy of the entire ANPR system (roughly 40 billion reads originally set up for the Olympics known as the 'Olympic Feed').

The original retention period for ANPR data was three years and the police are discussing extending this to 7-10 years. The retention period seems to be in flux and the debate about extending it in private without informing the driving public nor parliament. It is unclear to my mind that, if the position were before the Information Tribunal it would be upheld as lawful given the volume of data (maybe 5 billion reads of innocent people's car movement) held beyond its original three year period.

Governance structures of ANPR do not appear as strong as the scale of the system might warrant (the DPA and a committee of ANPR users involving the ICO, the SCC and HO). I have spoken to officers who run the system who would welcome stronger governance and I have no evidence of wrong doing.

I should be surprised if the agencies through NTAC do not also hold of copy of the ANPR for CT purposes. But this is not avowed. Paradoxically, if the bill comes into force and such a copy of ANPR were avowed as a Bulk Personal Data Set then the governance regime as set out in the draft Bill would be far stronger than that governing the original data. In recent weeks I have written publicly to Sir Bernard Hogan Howe, Tony Porter and my work has been covered by the Sunday Times and the Guardian – see my blog posts http://talkaboutlocal.org.uk/tag/anpr/ . Sources suggest that this exposure has revealed that ANPR has not been slotted into the draft Bill framework. The lack of a settled retention policy for the main ANPR system and the unusual governance

The Committee examines the Home Secretary on Wednesday and I wonder if this could be an opportunity to ascertain whether the agencies hold a copy of the ANPR database for CT purposes, whether this will be regarded as a Bulk Personal Data Set, what it is for and what the data retention period is?

10 January 2016

Simon Pooley—written evidence (IPB0060)

1. Background

I am a UK citizen who has worked developing software for computers and communication devices since the early 1980s. I was an "early adopter" of the internet for professional and private purposes, and have followed its development and take up with great interest.

My overall view of the Draft Investigatory Powers Bill is that it is unnecessary, disproportionate and technically ill-thought-out.

Thank you for this opportunity to comment. I am basing my response on the structure of the questions suggested by the Committee's "Call for Written Evidence"

2. Overarching/thematic questions:

2.1 Are the powers sought necessary?

No, the case has not been made. No evidence has been presented as to how the powers made available under the draft bill will be used by security services to prevent terrorism or other criminal activity. The oft-quoted example of using ICRs (Internet Connection Records) to track a missing person is at best misleading, and maybe disingenuous: the missing person's communication devices will simply indicate that they have been continually connected to a variety of social media sites, and investigators would far better direct their efforts to the organisations running those sites.

2.2 Are the powers sought legal?

As a general point, a government should not collect potentially private and personal data on its citizens, even in bulk and anonymised, without unambiguous justification.

The loose and unworkable "definition" of ICRs in the Draft Bill will mean that a significant amount of legal testing in the courts will be needed to clarify the meaning and intention of the bill. This is bad for justice.

2.3 Are the powers sought workable and carefully defined?

No. In particular the notion of an ICR is not adequately defined. See "Communications Data", below.

2.4 Are the powers sought sufficiently supervised?

No. As currently drafted, the Home Secretary is the primary supervisor. Retention and Interception Orders should only be issued with judicial authority. Whatever the stated intentions of the current Home Secretary, a future holder of that position may act differently. This is surely fundamental to the operation of a democracy.

3. Specific questions:

3.1 General

Security, Intelligence and Law Enforcement services should have the powers for **targeted** surveillance and interception, with judicial oversight.

3.2 Interception

Whilst I believe there is sufficient justification for targeted interception, there is none for bulk interception of individuals' personal private communications data.

Individuals will always be able to communicate in confidence using pre-agreed code signals, and with minor inconvenience will be able to continue to use the internet through VPNs https://en.wikipedia.org/wiki/Virtual_private_network or systems designed to avoid interception such as Tor https://en.wikipedia.org/wiki/Tor_(anonymity_network)

3.3 Communications Data

The idea of an ICR (Internet Connection Record" is not adequately defined (See written evidence from Adrian Kennard, Andrews & Arnold Ltd, 10th Dec 2015).

Because of the incomplete definitions of what is required, Service and Communications Providers are unable to adequately cost the development of the equipment and ongoing running costs necessary to satisfy the requirements of the bill.

3.4 Data Retention

Due to the way the internet works (again, see written evidence from Adrian Kennard, Andrews & Arnold Ltd, 10th Dec 2015), ICRs are unlikely to be consistent and will not be particularly useful.

Attempting to use IP addresses to identify individual "persons of interest" is not straightforward, due to shared use of IP addressed and complexities of "Carrier Grade NAT" (see https://en.wikipedia.org/wiki/Carrier-grade_NAT).

3.5 Equipment Interference

Powers to interfere with commercially available telecommunications equipment should not be given to government or their agents. This will harm commercial interests and will give the UK a reputation as a country that does not allow organisations or individuals to communicate confidentially.

3.6 Bulk Personal Data

The collection of vast quantities of communications data records is likely to create a hugely attractive target for hackers. With this data being captured, logged and maintained in a variety of different ways by different service providers, it is quite likely to be compromised at some point in the future (e.g. a "Snowden"-like individual leaking the data or a "Talk Talk"-style data breach).

The Draft Bill is inadequate in its description of "Request Filters" – it is sufficiently vague that the Home Office could subsequently change scope of information collated and returned. The

idea of external programmatic access to intercepted data provides a weakness which will be a target of hacking.

The Draft Bill does not clearly define what will be collected, and for what purpose. The Code of Practice is not published. Retention Notices will be secret and cannot be shared between Communication Providers, so there will be little commonality about what data will be captured, and how.

3.7 Oversight

The judiciary should be in overall charge of authorizing individual, targeted interception and retention orders before they occur. Post-act oversight is a poor compromise in a democracy.

20 December 2015

Privacy International—written evidence (IPB0120)

Summary

1. Thank you for the opportunity to provide comments on the draft Investigatory Powers Bill (IP Bill).

2. Privacy International was founded in 1990. It is a leading charity promoting the right to privacy across the world. It is based in London and, within its range of activities, focuses on tackling the unlawful use of surveillance. It is frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has advised, and reported to, among others, the Council of Europe, the European Parliament, the Organisation for Economic Co-operation and Development, and the United Nations.

3. The IP Bill aims to overhaul existing surveillance legislation and act as an example of the "gold standard" for governments around the world. Unfortunately, the current draft falls significantly short of this goal.

4. In doing so, the IP Bill, as currently drafted, violates the right to privacy (under UK and international human rights law); undermines the security of digital data; imposes burdensome and unreasonable requirements on companies; and erodes the trust of individuals in communication technologies. It does all this while, at the same time, failing to provide an accessible, foreseeable legal framework that would make intelligence agencies and the police accountable for their surveillance activities; or providing for an oversight framework which - while in some ways improves upon the current regime - still does not have the necessary powers to check and prevent abuse.

5. The following are some highlights of our concerns and recommendations, which are more fully described throughout this submission:

6. Bulk warrants – Parts 6 and 7 of the draft IP Bill address a range of bulk warrants: bulk interception warrants; bulk acquisition warrants; bulk equipment interference warrants; and bulk personal dataset warrants. We have expressed our concern that such warrants would codify a practice of mass, untargeted surveillance.[1091] This practice subverts the traditional investigative process, by which the Government has reason to suspect someone and applies for a warrant to surveil that person.[1092] Bulk warrants, by contrast, permit the intelligence agencies to surveil everyone. They are neither lawful, nor necessary or proportionate. Nor have they proven to be effective. Privacy International calls for their removal from the IP Bill.

7. Thematic warrants – While disguised as targeted surveillance, the IP Bill seeks to introduce in law "thematic warrants" (both for interception and equipment

1091 *See* Privacy International & Open Rights Group, Submission to the Joint Committee on Human Rights on the Draft Investigatory Powers Bill, 7 Dec. 2015, para. 9 [hereinafter "Joint Committee on Human Rights Submission"], available at http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/human-rights-committee/legislative-scrutiny-draft-investigatory-powers-bill/written/25654.pdf; *see also* Anderson Report, para. 2.31 ("Bulk collection of electronic messages, as the Snowden Documents brought home, can be achieved with far less effort and so brings the potential (if not properly regulated) for spying on a truly industrial scale.").

1092 Bruce Schneier, Data and Goliath (2015), page 179.

interference.) Thematic warrants delegate the choice as to whose privacy will be interfered with to the police or intelligence agencies, increasing the risk of arbitrary action and undermining the implementation of effective judicial authorisation. Communications or equipment *within* the United Kingdom may be intercepted or interfered with under a thematic warrant. These are bulk powers being used against people within the UK. Privacy International calls for their removal from the IP Bill.

8. Communications data and data retention – Even the Home Office admits that these parts of the IP Bill contain new powers. In fact, they significantly expand the capacity of a range of public authorities (not only the intelligence services and the police) to obtain highly sensitive information about individuals without judicial authorisation. Internet Connection Records (ICRs), while far from clear in scope, have the potential to intrude significantly into people's private lives. This is combined with a regime of blanket, untargeted data retention that, if adopted, will lead to the collection and storage, for up to a year, of highly revealing information pertaining to virtually all communications sent, received or otherwise created by us all. Privacy International opposes blanket data retention and suggests the introduction of targeted preservation orders instead.

9. Equipment interference – The IP Bill seeks to introduce "equipment interference" powers, including in bulk. Hacking is an incredibly intrusive form of surveillance, permitting both real-time surveillance as well as access to the breadth of private information we increasingly store on our digital devices, from text messages and emails to photos, videos, address books and calendars. Moreover, hacking, as undertaken by any actor, including the state, fundamentally impacts on the security of computers and the internet. For these reasons, we question whether hacking can ever be a legitimate aspect of state surveillance.

10. Privacy International submitted oral evidence to the Joint Committee on 9 December 2015. In this submission, Privacy International builds on the information provided during that hearing and provides responses to all the questions posed by the Joint Committee in its call for written evidence.[1093]

Overarching/thematic questions

Are the powers sought necessary?

11. This question has two dimensions – efficacy and legality. Privacy International submits that for certain of the parts of the IP Bill, particularly the bulk powers and data retention, necessity has not been demonstrated on either dimension.

Has the case been made, both for the new powers and for the restated and clarified existing powers?

1093 Privacy International also submitted written evidence on the IP Bill to the Science and Technology Committee of the House of Commons (available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25170.html) and the Joint Committee on Human Rights (available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/human-rights-committee/legislative-scrutiny-draft-investigatory-powers-bill/written/25654.pdf).

12. We dispute the UK Government's characterisation of particular powers as "existing" rather than "new". The foreword to the draft IP Bill by the Home Secretary states, for example, that "[t]he draft Bill only proposes to enhance powers in one area – that of communications data retention".[1094] The distinction between "new" and "existing" powers is important because "new" powers are often subjected to a higher level of scrutiny. By erroneously describing "new" powers as "existing", the Government seems to be seeking easier acceptance of new and/or enhanced powers that should be subject to especially critical analysis and robust debate.

13. One particularly glaring example of this mischaracterisation concerns the "equipment interference" power. Privacy International's current complaint before the Investigatory Powers Tribunal (IPT), which asserts that GCHQ has violated the Computer Misuse Act (CMA) 1990 and the European Convention on Human Rights (ECHR) by hacking computers, is instructive on this point.[1095] Until we brought our claim, GCHQ had never publicly acknowledged engaging in equipment interference.[1096] After we filed our complaint, the Home Office published a draft Equipment Interference Code of Practice[1097] in an apparent attempt to provide the legal specificity necessary to address our assertion any hacking the intelligence services were conducting was not "in accordance with law." Yet the draft Code is not primary legislation.

14. The draft IP Bill places the power to hack on statutory footing for the first time.[1098] In such circumstances, we submit that this power cannot be characterised as "existing".

15. *New Powers* - Below, we detail how the operational case for the following new powers has not been made: bulk warrants; communications data, with respect to (a) ICRs and (b) data retention; and equipment interference.

16. <u>Bulk Warrants - Efficacy:</u> The primary operational justification for bulk warrants is to improve knowledge of threats to national security through the detection of patterns

---

1094 Foreword, Investigatory Powers Bill.

1095 The Snowden documents indicate that GCHQ had, at least internally, arrived at a similar conclusion. A September 2010 document prepared by a GCHQ representative reports a "concern" that a certain hacking technique "may be illegal" because

> The Computer Misuse Act 1990 provides legislative protection against unauthorised access to and modification of computer material. The act makes specific provisions for law enforcement agencies to access computer material under powers of inspection, search or seizure. However, the act makes no such provision for modification of computer material.

Privacy International et al. v. Secretary of State for Foreign and Commonwealth Affairs, Skeleton Argument Served on behalf of the Claimants, para. 23, 7 Oct. 2015 [hereinafter "Skeleton Argument"].

1096 *See* Anderson Report, paras. 7.64-5, 14.13.

1097 The draft Equipment Interference Code of Practice is available at: https://www.gov.uk/government/publications/interception-of-communications-and-equipment-interference-codes-of-practice

1098 *See* Anderson Report, para 12.8 (noting that "the use of [equipment interference], only recently acknowledged by the Government through the publication of the Draft Equipment Interference Code" was one of several "intrusive practices" that "do not find clear and explicit basis in legislation"). The pre-existing legislation that the Home Office cites as authorizing hacking – the Intelligence Service Act 1994 and the Police Act 1997 – both do not mention equipment interference. Instead, they provide broad powers under which, as Anderson declares, it is not at all clear hacking would be carried out.

and links in communications data.[1099] The Government has represented that it needs "to sift through 'haystack' sources – without looking at the vast majority of material that has been collected – in order to identify and combine the 'needles', which allow them to build an intelligence picture."[1100]

17. This operational argument is subject to critical fallacies that we encourage the Committee to seriously consider. The success of data mining relies on a set of particular factors, including "a well-defined profile", "a reasonable number of events per year", and a low "cost of false alarms".[1101] For this reason, credit card fraud detection, for example, has become a relatively effective form of data mining: fraudulent purchases are easy to identify, credit card transactions number in the billions and the cost of a false alarm is a phone call to the cardholder.

18. By contrast, terrorist plots are rare and each has unique facets, meaning "false positives completely overwhelm the system."[1102] And the cost of a false alarm is high, leading to time and money wasted following false leads when our intelligence agencies could be doing more productive work. We see this in the American context: reviews of the NSA's mass surveillance programs have concluded that they were "not essential to preventing attacks" or had "no discernible impact".[1103] A recent Council of Europe report came to the same conclusion this year, finding that "mass surveillance is not . . . effective as a tool in the fight against terrorism and organised crime, in comparison with traditional targeted surveillance."[1104]

19. As security expert Bruce Schneier puts it:

> When you're looking for the needle, the last thing you want to do is pile lots more hay on it. More specifically, there is no scientific rationale for believing that adding irrelevant data about innocent people makes it easier to find a

---

1099 See the Home Office Factsheets on "Bulk Interception", "Bulk Communications Data", "Bulk Equipment Interference", and "Bulk Personal Databases", all available at https://www.gov.uk/government/publications/draft-investigatory-powers-bill-overarching-documents. *See also* ISC Report, para. 90 ("GCHQ's bulk interception capability is used primarily to find patterns in, or characteristics of, online communications which indicate involvement in threats to national security.").

1100 *See* ISC Report, para. 51 (quoting written evidence submitted by the Government); *see also* Anderson Report, para. 10.22(a).

1101 *Id*.

1102 *Id*. at page 137 (citing, *inter alia*, John Mueller and Mark G. Stewart, Terror, Security, and Money: Balancing the Risks, Benefit, and Costs of Homeland Security, Oxford University Press (2011), chap. 2; G. Stuart Mendenhall & Mark Schmidhofer, "Screening Tests for Terrorism", *Regulation*, Winter 2012-13, http://object.cato.org/sites/cato.org/files/serials/files/regulation/2013/1/v35n4-4.pdf; Fred H. Cate, "Government data mining: The need for a legal framework", Harvard Civil Rights-Civil Liberties Law Review 43, Summer 2008, http://www.law.harvard.edu/students/orgs/crcl/vol43_2/435-490_Cate.pdf; Jeff Jonas & Jim Harper, "Effective counterterrorism and the limited role of predictive data mining", Cato Institute, 11 Dec. 2006, http://www.cato.org/publications/policy-analysis/effective-counterterrorism-limited-role-predictive-data-mining); *see also* ISC Report, para. 56 ("Amongst the everyday internet usage of billions of people . . . a very small proportion will relate to threats to the national security of the UK and our allies.").

1103 Peter Bergen, "Do NSA's Bulk Surveillance Programs Stop Terrorists?", New America Foundation, Jan. 2014, https://www.newamerica.org/international-security/do-nsas-bulk-surveillance-programs-stop-terrorists/; The President's Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World, Dec. 2013, page 104; *see also* Yochai Benkler, "Fact: The NSA Gets Negligible Intel from Americans' metadata. So end collection", Guardian, 8 Oct. 2013, http://www.theguardian.com/commentisfree/2013/oct/08/nsa-bulk-metadata-surveillance-intelligence.

1104 PACE Committee on Legal Affairs and Human Rights, *Mass Surveillance* (Jan. 2015), at para. 126, available at http://website-pace.net/documents/19838/1085720/20150126-MassSurveillance-EN.pdf.

> terrorist attack, and lots of evidence that it does not. You might be adding slightly more signal, but you're also adding much more noise.[1105]

20. Mass surveillance is the wrong tool for ferreting out criminals and terrorists. Pouring more resources into these programs results in less security for us all.[1106] We are awash with examples of how terrorist plots have been or could have been detected using time-honoured investigative techniques.[1107] The RUSI report indicates that "lack of detailed intelligence available on a small number of high-priority targets . . . is the prime concern, rather than broader intelligence available on a large number of low-priority targets.[1108]

21. Both the Anderson and ISC Reports cite case studies provided by GCHQ, which supposedly demonstrate the efficacy of bulk capabilities.[1109] These case studies cannot be published, even in redacted form, which makes it difficult for the public to independently evaluate the efficacy argument.[1110] Anderson himself notes that "[t]here are limits to what the public will (or should) take on trust" and that "the justification to a public audience of such a potentially intrusive power deserves and arguably needs more".[1111] The Government has thus far failed to provide more. We therefore encourage the Committee to closely scrutinise arguments that these tactics are operationally necessary, including by considering the actual value of information produced by mass surveillance and how much of this information could have been obtained by less intrusive means.

22. Internet Connection Records (ICRs) – Efficacy: The "great majority of communications data use is for the prevention or detection of crime, or the prevention of disorder", followed by national security and emergency prevention of death or injury.[1112] The Government represents that ICRs "are records of the internet services that have been accessed by a device" and the power to collect them is necessary "to attribute a particular action on the internet to an individual person."[1113] It provides, as an example of an ICR, "a record of the fact that a smartphone had accessed a particular

---

1105 Schneier, Data and Goliath, page 138 (citing Mike Masnick, "Latest Revelations Show How Collecting All the Haystacks to Find the Needle Makes the NSA's Job Harder", Tech Dirt, 15 Oct. 2013, https://www.techdirt.com/articles/20131014/17303424880/latest-revelations-show-how-collecting-all-haystacks-to-find-data-makes-nsas-job-harder.shtml; Chris Young, "Military intelligence redefined: Big Data in the battlefield", Forbes, 12 Mar. 2012, http://www.forbes.com/sites/techonomy/2012/03/12/military-intelligence-redefined-big-data-in-the-battlefield/).

1106 *See* Jeffrey W. Seifert, "Data Mining and Homeland Security: An Overview", Congressional Research Service, 3 Apr. 2008, https://fas.org/sgp/crs/homesec/RL31798.pdf.

1107 National Commission on Terrorist Attacks, The 9/11 Commission Report: Final Report of the National Commission on Terrorist Activities upon the United States, https://www.gpo.gov/fdsys/pkg/GPO-911REPORT/pdf/GPO-911REPORT.pdf. Simon Shuster, "The Brothers Tsarnaev: Clues to the Motives of the Alleged Boston Bombers", Time, 19 Apr. 2013, http://world.time.com/2013/04/19/the-brothers-tsarnaevs-motives/.

1108 RUSI Report, para. 3.53.

1109 Anderson Report, para. 7.26; ISC Report, para. 81.

1110 Anderson Report, para. 7.26; ISC Report, para. 81. Anderson annexed six outline examples of these case studies to his report, but describes this effort as only "go[ing] a little way towards remedying th[e] defect" of lack of public transparency. Anderson Report, para. 7.27.

1111 Anderson Report, paras. 7.27, 10.8.

1112 Anderson Report, para. 9.21.

1113 Home Office, "Factsheet: Internet Connection Records", https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473745/Factsheet-Internet_Connection_Records.pdf.

social media website at a particular time."[1114]

23. The precise definition of an ICR remains unclear but appears to include the "web logs" addressed by Anderson.[1115] In his report, Anderson noted that "web log" was also an uncertain term but quoted the Home Office's definition:

> "Weblogs are a record of the interaction that a user of the internet has with other computers connected to the internet. This will include websites visited up to the first '/' of its [url], but not a detailed record of all web pages that a user has accessed. This record will contain times of contacts and the addresses of the other computers or services with which contact occurred."[1116]

24. Anderson concluded that "[u]nder this definition, a web log would reveal that a user has visited e.g. www.google.com or www.bbc.co.uk, but not the specific page."[1117]

25. The equivalence between ICR and "web log" is important because Anderson expressed deep hesitation about introducing an obligation for CSPs to retain such data. He noted it had not been demonstrated that "access to weblogs is essential for a wide range of investigations" and that even within the law enforcement community, "it is widely accepted . . . that the compulsory retention of web logs would be potentially intrusive."[1118] From a comparative perspective, Anderson observed that no other European or Commonwealth country appears to compel their CSPs to retain such data and that Canadian and American law enforcement represented "that there would be constitutional difficulties in such a proposal."[1119] He concluded that while "retained records of user interaction with the internet (whether or not via web logs) would be useful . . . that is not enough on its own to justify the introduction of a new obligation on CSPs, particularly one which could be portrayed as potentially very intrusive on their customers' activities."[1120]

26. Anderson emphasised that any proposal progressing this issue would "need to be carefully thought through and road-tested with law enforcement, legal advisers and CSPs" with robust consultations with "[o]utside technical experts, NGOs and the public".[1121] He suggested a detailed list of issues that should be addressed, including, *inter alia*:

    A. the precise definition of the purposes for which such records should be accessible, and the relative importance of those purposes;

    B. the extent to which those purposes can in practice be achieved under existing powers (e.g. the inspection of a seized device), by less intrusive measures than

---

1114 *Id*.

1115 See Investigatory Powers Bill, Explanatory Notes, para. 190, which describes ICRs in language that is similar to Anderson's description of web logs. It is not clear, however, that paragraph 190 is an accurate description of everything that could be captured under the IP Bill's definition of ICRs.

1116 Anderson Report, para. 9.53.

1117 *Id*. at para. 9.54.

1118 *Id*. at para. 9.60.

1119 *Id*. at para. 9.55.

1120 *Id*. at para. 14.33.

1121 *Id*. at para. 14.35.

that proposed or by data preservation, i.e. an instruction to CSPs to retain the web logs or equivalent of a given user who was already of interest to law enforcement;

C. the precise records that would need to be retained for the above purposes, and how those records should be defined;

D. the steps that would be needed to ensure the security of the data in the hands of the CSPs;

E. the implications for privacy; or

F. the cost and feasibility of implementing the proposals.[1122]

27. Privacy International notes that while the Home Office has produced a stand-alone document purporting to lay out the operational case for ICRs, it fails to address many of the questions outlined above.[1123] We accordingly encourage the Committee to press the Home Office on these points.

28. Data Retention- Efficacy: The primary operational justification for compulsory data retention comes from law enforcement agencies, who insist they need this power to preserve evidence of historic criminality.[1124] Privacy International does not dispute that older data can be important to criminal investigations; we simply submit that there are alternatives that may be just as effective but do not pose the same privacy intrusions or security risks as bulk retention. The serious security risks posed by the data retention requirements in the draft IP Bill are particularly acute.[1125] Precisely because of the revealing nature of such data, the database(s) where this retained data is stored are also likely to be targeted by cyber criminals and foreign intelligence services. By compelling retention, the Government "unnecessarily endangers the security of communications service providers who could be subject to increased attacks."[1126] In the past year, we have witnessed the ramifications of several such attacks on businesses such as TalkTalk, Vodafone and British Gas.[1127] In a study commissioned by the Department of Business, Innovation and Skills, 90% of large businesses and 74% of small businesses had detected at least one breach in the previous twelve months.[1128]

29. We urge the Committee to press the Home Office on alternatives such as Data Preservation Orders for specific individuals based on an investigation or proceeding. The Home Office's answers should be concrete, focusing on issues such as relative efficacy, cost and intrusion on privacy. Finally, we remind the Committee that CSPs

---

[1122] *Id*. at para. 14.33.

1123 Home Office, "Operational Case for the Retention of Internet Connection Records", https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473769/Internet_Connection_Records_Evidence_Base.pdf.

1124 *See* Anderson Report, para. 9.45.

1125 Science & Tech Committee Submission, paras. 26-30.

1126 *Id*. at para. 29.

1127 *Id*. at para. 29 n. 17.

1128 Department of Business, Innovation and Skills, "2015 Information Security Breaches Survey", https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/432412/bis-15-302-information_security_breaches_survey_2015-full-report.pdf.

tend to keep customer data for their own business purposes so foregoing mandatory bulk retention will not mean that it will all disappear.

30. Equipment Interference - Efficacy: With respect to law enforcement, the Government has failed to make any operational case for the power to hack. The Government's factsheet on "Targeted Equipment Interference" is limited to sweeping statements – e.g., "helps law enforcement agencies to protect the most vulnerable members of society" – but makes no concrete arguments as to why such an intrusive surveillance technique is needed.[1129] For example, while the Government argues that hacking could assist in obtaining "a key piece of information encrypted in transmission", it has provided no evidence as to the number of times encryption has actually impeded a criminal investigation.[1130] As a point of comparison, the US government has reported that in 2013, encryption stymied the police just nine times, up from four in 2012.[1131]

31. The operational case for why the security and intelligence agencies require the power to hack is similarly weak. The only operational statement described by Anderson in terms of this capability is that the agencies "need to develop new methods of accessing data, for example through increased use of CNE."[1132] But there is no further elaboration on how necessary CNE is to the acquisition of operationally important data. The Government's factsheet points to the two following facts as support for the power to hack:[1133]

    1. During 2013 around 20% of GCHQ's intelligence reports contained information that derived from EI operations;

    2. MI5 has relied on EI in the overwhelming majority of high priority investigations over the past 12 months.

32. These two assertions fail to demonstrate that the potential intelligence benefits of hacking outweigh the critical security risks posed by this practice. The Government does not, for example, elaborate on the quality of "information that derived from EI operations" and whether that information could have been obtained by any other means. Similarly, it is unclear the extent to which EI was critical to the "high priority investigations" in which it played a role and again, the extent to which MI5 might rely on other techniques that expose the public to less of a security risk.

1129 Home Office, "Factsheet: Targeted Equipment Interference", https://www.gov.uk/government/publications/draft-investigatory-powers-bill-overarching-documents. Anderson records an equally vague statement from law enforcement agencies regarding their need for this power. *See* Anderson Report, para. 9.75.

1130 Home Office, "Factsheet: Targeted Equipment Interference".

1131 *See* Andy Greenberg, "Rising use of encryption foiled cops a record 9 times in 2013," *Wired*, 2 July 2014, http://www.wired.com/2014/07/rising-use-of-encryption-foiled-the-cops-a-record-9-times-in-2013/.

1132 Anderson Report, para. 10.21. The ISC Report is limited to describing the scope of current hacking operations. *See* ISC Report, paras. 173-78.

1133 Home Office, "Factsheet: Targeted Equipment Interference". The Home Office's Factsheet on "Bulk Equipment Interference" is even less helpful. Aside from reiterating the first statistic, it provides no additional substantive arguments in support of the hacking power. As we explained in our prior submission to the Science & Technology Committee, the bulk equipment interference powers compound the security concerns presented by targeted hacking by giving "almost unfettered powers to the intelligence services to decide who and when to hack." Science & Tech Committee Submission, para. 18.

33. Existing Powers - Even if the Government were to insist that the powers we characterise as "new" are "existing", Privacy International submits that the efficacy and legality concerns outlined above remain relevant and are reason enough to seriously question the inclusion of such powers in the draft IP Bill.

34. We also submit that with respect to existing powers, the draft IP Bill proposes expanding some of them. Below, we describe how the case has not been made for one such expansion: the use of "thematic warrants" under targeted interception as reflected in the expansion of the subject matter of warrants in IP Bill clause 13.

35. The ISC Report revealed for the first time that the Home Secretary has been interpreting "person" in the Regulation of Investigatory Powers Act 2000 (RIPA) section 8(1)(a) as "any organisation or any association or combination of persons".[1134] MI5 has been, in practice, obtaining "thematic warrants" in reliance on this definition.[1135] We address the legal concerns surrounding thematic warrants in more detail in paragraphs 67 to 77 below. Given the very recent avowal of thematic warrants and the shaky interpretation of RIPA upon which they rest, we submit that thematic warrants should be considered an expansion of the targeted interception authorised under RIPA.[1136]

36. Efficacy: The operational case for such an expansion is not clear. The ISC indicates that "the very significant majority of 8(1) warrants relate to one individual" while "in some limited circumstances an 8(1) warrant may be thematic."[1137] MI5 explained to the ISC that it applies for a thematic warrant "where we need to use the same capability on multiple occasions against a defined group or network on the basis of a consistent necessity and proportionality case . . . rather than [applying for] individual warrants against each member of the group."[1138] This explanation suggests a thematic warrant is a matter of convenience – resulting in certain efficiency gains – rather than of operational necessity. This reading is borne out by law enforcement's representation to Anderson that thematic warrants would help to deal with the proliferation of documents required by the current warrant regime.[1139] It is worth underlining that the Interception of Communications Commissioner's Office represented to the ISC that, in some instances, thematic warrants have been abused.[1140] The ISC itself expressed, in its conclusion, reservations about "the extent that this capability is used and the associated safeguards."[1141]

37. Recommendations

    1. Remove bulk powers from the draft IP Bill.

1134 ISC Report, para. 42.

1135 *Id*. at para. 43; Anderson Report, para. 6.42.

1136 Anderson Report, para. 14.62 (noting that there is "no very clear backing for [thematic warrants] on the face of RIPA s8(1)).

1137 ISC Report, para. 43.

1138 *Id*. at para. 43 (quoting written evidence submitted by MI5).

1139 Anderson Report, para. 9.33 (quoting the law enforcement agencies' complaint of "so many pieces of paper on the same target: different routes, different authorisation levels, not much flexibility of timescale").

1140 ISC Report, para. 45.

1141 *Id*. at ISC, page 24, para. D; *see also* Anderson Report, para. 7.16(a) (describing the ISC as viewing thematic warrants "warily").

2. Remove ICRs as a category of communications data that can be collected or ordered retained from the draft IP Bill.

3. Remove the obligation to retain communications data in the draft IP Bill, replacing it with the ability to issue targeted preservation orders based on individualized suspicion.

4. Carefully assess whether the operational case for including equipment interference in the draft IP Bill outweighs the security concerns raised by government use of equipment interference.

5. Remove Clause 13(2), which permits the Government to apply for "thematic warrants" under the targeted interception power, from the draft IP Bill.

Are the powers sought legal? Are the powers compatible with the Human Rights Act and the ECHR?

38. The fact that the IP Bill seeks to put on a statutory footing the surveillance powers exercised by the intelligence services and law enforcement does not, in itself, fulfil the requirements of legality under international human rights law.

39. Article 8 of the ECHR requires certain minimum safeguards in the legal framework regulating surveillance activities to protect against arbitrary interference with privacy and abuse. In particular, the law must include the nature of the offences which may give rise to an order to interfere with someone's privacy; a definition of the categories of people liable to have their communications (including communications data) monitored; a limit on the duration of such monitoring; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when sharing the data with other parties; and the circumstances in which the data obtained must be erased or destroyed.[1142]

40. That the data sought may be of value is not sufficient to make its collection or retention lawful. For instance, in S and Marper v United Kingdom, the UK government submitted that the retention of DNA samples from people who had not been charged or convicted of a criminal offence was of "inestimable value" and produced "enormous" benefits in the fight against crime and terrorism (§92). The Grand Chamber of the ECtHR nonetheless held that the retention was a "disproportionate interference" with those individuals' private lives (§135). Central to the reasoning was the absence of any assessment of suspicion by the authorities that was sufficient to justify the retention of each individual's DNA data.[1143]

41. Furthermore, in October 2015, the Grand Chamber of the Court of Justice of the European Union (CJEU) ruled that "legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for

1142 See Zakharov v Russian Federation, [GC], No. 47142/06, 4 December 2015, confirming earlier jurisprudence of the Court.

1143 See S and Marper v United Kingdom, [GC] No. 30562/04, 4 December 2008.

private life."[1144]

42. Given this, Privacy International believes the bulk warrants in the draft IP Bill are unlawful (Parts 6 and 7 of the IP Bill). Similar concerns apply to the proposed regime for retention of communications data (Part 4 of the IP Bill). We have expressed certain of our concerns regarding legality in our joint submission with Open Rights Group to the Joint Committee on Human Rights.[1145] We expand upon that submission here.

Bulk Warrants

43. Targeting - Bulk warrants do not require any suspicion whatsoever on the part of the authorities that a person has committed a criminal offence or is a threat to the interests of national security (or other relevant grounds.) Similarly these warrants do not have to define the categories of persons who are liable to have their communications monitored. Instead bulk warrants need only state the operational purposes for which data is to be obtained, and the IP Bill expressly notes that these can be "general purposes", thereby potentially being as broad as "countering terrorism" (see in particular Clauses 111(4), 125(4) and 140(5)).

44. In this respect, the IP Bill does not address the concerns raised by the current "bulk" warrant regime under RIPA, which this bill aims to reform. As noted by the ISC in relation to the RIPA regime: "[T]he categories are expressed in very general terms. For example: 'Material providing intelligence on terrorism (as defined by the Terrorism Act 2000 (as amended)), including, but not limited to, terrorist organisations, terrorists, active sympathisers, attack planning, fund-raising.'"[1146]

45. Further, nowhere in the IP Bill is there a definition of "national security" or "economic well-being" of the United Kingdom (grounds under which bulk warrants can be issued), nor any indication of the circumstances under which communications can be surveilled on the basis of such grounds. It leaves authorities an almost unlimited degree of discretion in determining which events are relevant to national security and does not require any assessment of the level of threat to justify secret surveillance.

46. As we discuss in our response to the question, "Is the authorisation process appropriate?", the broad scope of the "bulk" warrants means the authorisation process falls short of what is required under international human rights law. In particular it leaves the authorities (including the Judicial Commissioners) unable to verify, as recently reiterated by the European Court of Human Rights in Zakharov, "the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to

---

1144 Judgment in Case C-362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015.

1145 See Privacy International and Open Rights Group's Submission to the Joint Committee on Human Rights on the Draft Investigatory Powers Bill, submitted 7 December 2015, available at http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/human-rights-committee/legislative-scrutiny-draft-investigatory-powers-bill/written/25654.pdf

1146 Intelligence and Security Committee of Parliament, report: Privacy and Security: A modern and transparent legal framework, 12 March 2015 para 101.

secret surveillance measures, such as, for example, acts endangering national security." [1147] Nor it will allow them to "ascertain whether the requested interception meets the requirement of 'necessity in a democratic society', as provided by Article 8 § 2 of the [ECHR], including whether it is proportionate to the legitimate aims pursued, by verifying, for example whether it is possible to achieve the aims by less restrictive means."[1148]

47. Renewal - "Bulk" warrants can be renewed an indefinite number of times (see Clauses 113, 127, 142, 161) and as there is no requirement to target a particular individual or premises, there is no restriction on the possibility that a person's communications may be routinely intercepted, again and again, for an indefinite period under successive "bulk" warrants.

48. Safeguards - The procedure to be followed for examining, sharing, retaining and deleting material or data obtained through "bulk" warrants are too broad and vague to provide sufficient guidance and prevent abuse.[1149]

49. In particular, the disclosure and copying of information obtained under a "bulk" warrant is broadly permitted so long as the information is or *is likely* to become necessary in the interests of national security or other relevant grounds. Similarly provisions regulating the destruction of material or data obtained through "bulk" warrants would allow the retention of such data indefinitely. Notably, these provisions do not limit copying, sharing or retaining data as necessary for the ground for which the specific warrant was originally issued, but for any grounds under which the "bulk" warrants can be issued.

50. There are no details on the safeguards required for the storage of data collected, with relevant Clauses of the IP Bill simply stating that such storage is done in "a secure manner".

51. The "safeguards" for examination of intercepted materials under "bulk" interception warrants confirm the discriminatory distinction already contained in the Regulation of Investigatory Powers Act (RIPA) between materials referable to an individual in the British Islands or not. For materials not related to individuals in the UK, there is no requirement of a targeted examination warrant. Instead, the intercepted materials can be examined without limitation, in so far as it is necessary for the purpose specified in the bulk warrant, which can be very general (Clause 119). A similar provision applies for bulk equipment interference warrants (Clause 147).

52. This distinction between external and internal communications is discriminatory on grounds of nationality and national origin.[1150] Further, as noted by David Anderson in

1147 Zakharov v Russian Federation, [GC], No. 47142/06, 4 December 2015, paragraph 260.

1148 Zakharov v Russian Federation, [GC], No. 47142/06, 4 December 2015, paragraph 261.

1149 See"general safeguards" under Clauses 117, 131, and 146.

1150 The UN High Commissioner for Human Rights and the UN Special Rapporteur on counter-terrorism and human rights have noted how several legal regimes on interception of personal communications, like the UK, distinguish between obligations owed to nationals and non-nationals and residents and non-residents, providing external communications with lower or non-existent protection, in ways that are discriminatory and incompatible with Article 26 of the ICCPR. See report of the UN High Commissioner on Human Rights on the right to privacy in the digital age, UN doc. A/HRC/27/37, 30 June 2014; and report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN doc. A/69/397, 23 September 2014.

his report A Question of Trust, the distinction between internal and external communications is arbitrary and rendered meaningless in the context of the technical architecture of modern digital communications, with messages such as e-mails routed through different countries even if both the sender and the intended recipient are resident in the UK.[1151]

53. Transferring data overseas - The "safeguards" that apply to transferring data to parties overseas are even weaker than those applicable for "domestic" sharing and leave wide discretion, only requiring the Secretary of State or another relevant authority to apply the already vague standards applicable to domestic sharing "to the extent (if any) as the Secretary of State consider appropriate".[1152] As such, any restrictions on the sharing of the collected data with foreign authorities are entirely at the discretion of the Secretary of State.

54. Privacy International is also concerned that the IP Bill fails to specify the circumstances in which such overseas transfer can be authorised. Except for the provisions regulating Mutual Assistance Warrants (that apply only to interception of communications) there is no mention in the IP Bill of the grounds, limits and authorisations required for sharing data obtained through surveillance. In this respect the IP Bill fails to resolve one of the most controversial and concerning practices of UK intelligence agencies, namely receiving and sharing acquired data in ways that are unregulated and may have the effect of circumventing applicable safeguards (notably under the Five Eyes arrangements). If confirmed, this would leave a significant loophole in the new regime regulating the use and oversight of investigatory powers, resulting in significant risks of abuse.[1153]

Data Retention

55. In our submission to the Joint Committee on Human Rights, we explained the extensive legal concerns raised by the communications data provisions in the draft IP Bill, including those on ICRs.[1154] We noted that the CJEU, ECtHR, and numerous UN human rights experts have recognised that the interception, collection and use of communications data interferes with the right to privacy.[1155] We also criticised provisions of the draft IP Bill that permit public authorities, with few exceptions, to obtain communications data without prior judicial authorisation.[1156] We further point the Committee to Open Rights Group's submission to the Science and Technology Committee, which explains why the operational case made by the Government falls short of demonstrating the necessity and proportionality of the communications data provisions.[1157] Finally, we highlight that, with respect to ICRs, Anderson observed that

1151 David Anderson QC, A Question of Trust, June 2015.
1152 See Clauses 118(2); 131(9); 146(9).
1153 See in this respect David Anderson's report, A question of trust, in particular recommendations 76 to 78.
1154 Joint Committee on Human Rights Submission, paras. 23-31.
1155 *Id*. at para. 29.
1156 *Id*. at para. 52.
1157 Written evidence submitted by Open Rights Group (IPB0034), http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25147.html.

their legality remains in serious question.[1158]

56. In our submission to the Joint Committee on Human Rights, we highlighted that the draft IP Bill's communications data retention regime violates existing EU provisions protecting the right to privacy, such as the Data Protection Directive 1995/46 and the Directive on privacy and electronic communications 2002/58/EC.[1159] We also noted that the regime appears to run afoul of the CJEU's ruling in *Digital Rights Ireland*, which struck down the 2006 Data Retention Directive.[1160] We emphasised that the draft IP Bill's provisions go much further than the invalidated EU Directive in several respects. We also highlighted that the lack of judicial authorisation required for data retention notices seems to flout language in *Digital Rights Ireland* describing the necessary review prior to government access to retained data.[1161] Finally, we described how these provisions are in breach of Article 8 of the ECHR as they exceed what could reasonably be regarded as "necessary in a democratic society".[1162] In short, the draft IP Bill's data retention requirements are likely to be subject to legal challenge based on recent judgments.

57. Recommendations

    1. Delete Parts 6 & 7 of the IP Bill related to "bulk warrants" and amend other Clauses accordingly.

    2. Remove the obligation to retain communications data in the draft IP Bill, replacing it with the ability to issue targeted preservation orders based on individualized suspicion.

58. Questions

    1. Ask the Home Office to clarify whether the IP Bill seeks to regulate intelligence sharing; if so how; and if not, why not?

Is the requirement that they be exercised only when necessary and proportionate fully addressed?

59. The fact that warrants and authorisations under the IP Bill can only be issued upon consideration that the measures are necessary and proportionate is not sufficient to ensure that such measures are indeed necessary to the pursuance of a legitimate aim.

60. Firstly, the warrant regime proposes a weak necessity test. The IP Bill specifies that the relevant authority, when assessing the necessity and proportionality of a proposed measure that will interfere with the right to privacy, should take into account "whether the information which it is considered necessary to obtain under

1158 Anderson Report, paras. 9.56, 9.60 ("[I]t is widely accepted within the law enforcement community that . . . the legal environment: *Digital Rights Ireland* may not be conducive to the imposition of such an extensive obligation").
1159 Joint Committee on Human Rights Submission, para. 34.
1160 *Id*. at para. 35.
1161 *Id*. at paras. 53-54.
1162 *Id*. at paras. 40-41.

the warrant could reasonably be obtained by other means."[1163]

61. This test falls short of requiring consideration of whether other less invasive techniques have been exhausted or would be futile, such that the techniques used is the least invasive option. It is a well-established principle under international human rights law that when contemplating a limitation to someone's right, the least invasive measure should be applied.[1164]

62. Secondly, the requirements of some of the warrants are so vaguely formulated that they will make it next to impossible to assess the necessity and proportionality of the envisaged measure. As noted above, the IP Bill allows the purposes of "bulk" warrants to be described in "general terms".

63. Even those supposedly "targeted" warrants (such as "targeted interception warrants" in Part 2 and "equipment interference warrants" in Part 5 of the IP Bill) would permit the intelligence services or law enforcement to conduct surveillance without needing to specify in the warrant the person or equipment that is to be the subject of the surveillance. As discussed in more detail below, in paragraphs 67 to 77, such "thematic" warrants could be broadly framed as targeting "a group of persons who share a common purpose or who carry on, or may carry on, a particular activity" (Clause 13); or "equipment belonging to, used by or in possession of persons who form a group that shares a common purpose or who carry on, or may be carrying on, a particular activity" (Clause 83).

64. This leaves almost unfettered discretion to the implementing authorities to decide who to put under surveillance and when. Notably, it makes it almost impossible for the Judicial Commissioner to assess whether the measures are necessary, in the absence of any requirement of reasonable suspicion.

Are [the powers sought] sufficiently clear and accessible on the face of the draft Bill?

65. It is difficult to address the almost two hundred pages of the IP Bill in this submission. As a general matter, however, while the IP Bill advances the conversation by setting out a number of powers in more detail than has previously been provided, it falls short of being clear and accessible. This is in part due to the collision of law and technology, which we address in more detail below in response to the question "Are the technological definitions accurate and meaningful (e.g. content vs communications data, ICRs etc.)?"

66. Yet there are several provisions to which technology is not central, but that nevertheless remain opaque.[1165]

67. <u>"Targeted" Interception and Equipment Interference</u> - Part 2 and Part 5 purport to permit "targeted" interception and equipment interference, respectively, in contrast

1163 See Clauses 14.6; 107.5; 122.4; and 137.4.

1164 See Zakharov v Russian Federation, [GC], No. 47142/06, 4 December 2015, paragraph 260; Human Rights Committee, in CCPR/C/21/Rev.1/Add.9 and report of the UN Special Rapporteur on counter-terrorism and human rights in A/HRC/13/37, para. 60.

1165 We note these provisions by way of example only.

to the "bulk" provisions of Part 6.

68. Describing Parts 2 and 5 as targeted is misleading. Both contain significant expansions of the subject matter of "targeted" warrants. This becomes apparent when we compare the new subject matter provisions (Clause 13 for interception and Clause 83 for equipment interference) with their immediate predecessors.

69. In RIPA, targeted interception is permitted under section 8(1) against "one person as the interception subject" or "a single set of premises." These provisions are broader than they appear on their face, as "person" is defined as "any organisation and any association or combination of persons" (RIPA section 81(1)).[1166] Nonetheless, there is an attempt at defining a specific target of the interception, especially with regard to premises.

70. The claimed predecessor to Part 5 is section 5 of the Intelligence Services Act 1994 (ISA). Section 5 permits a warrant to issue against "any property so specified" (ISA section 5(2)). Again, specificity is required.

71. Clauses 13 and 83, in contrast, allow interception and equipment interference warrants to relate to, among others:

    1. people or equipment "who share a common purpose or who carry on, or may carry on, a particular activity" (Clauses 13(2)(a) and 83(b));

    2. "more than one person or organization, or more than one set of premises, where the conduct authorized or required by the warrant is for the purposes of the same investigation or operation" (Clauses 13(2)(b) and 83(c)&(e));

    3. "equipment that is being, or may be used, for the purposes of a particular activity or activities of a particular description" (Clause 83(f)); or

    4. the "testing, maintenance or development" of capabilities relating to interception or equipment interference (Clauses 13(2)(c) and 83 (g)).

72. These subject matter expansions are apparently intended to encompass "thematic" warrants.[1167]

73. Under a thematic warrant, the Secretary of State and a Judicial Commissioner will not approve each individual target of the surveillance. Instead, the police and intelligence agencies can choose their targets without additional sign off. For instance, a thematic warrant might authorise the hacking of "all mobile phones in Birmingham" (Clause 83(e)) or the interception of the communications of "anyone suspected of having travelled to Turkey" (Clause 13(2)(a)).

74. Both the Interception of Communications Commissioner[1168] and the Intelligence

1166 This definition came to prominence when it was revealed in the Intelligence & Security Committee's report as the basis for issuing "thematic warrants," which are described in paragraphs 42 to 45 of that report. Intelligence and Security Committee of Parliament, *Privacy and Security: A modern and transparent legal framework* (12 March 2015), available at http://isc.independent.gov.uk/news-archive/12march2015 (hereinafter "ISC Report").

1167 Investigatory Powers Bill, Explanatory Notes, para. 212.

1168 ISC Report, para. 45.

Services Commissioner[1169] have expressed concerns about the use of such thematic warrants, especially when they become too broad. Such concern is understandable, given that thematic warrants delegate the choice as to whose privacy will be interfered with to the police or intelligence agents, increasing the risk of arbitrary action and undermining the implementation of effective judicial authorisation. As the Intelligence Services Commissioner points out, "the critical thing . . . is that the submission and the warrant must be set out in a way which allows the Secretary of State to make the decision on necessity and proportionality" (emphasis in original).[1170] As discussed above, thematic warrants make this very difficult, especially where the subject matter may be drawn as broadly as Clauses 13 and 83 would permit.[1171]

75. Thematic warrants also cut against deeply entrenched principles of the common law. A series of eighteenth century cases established the unconstitutionality of "general warrants", which permitted the Government to search and seize or arrest on the basis of classes of individuals. In Money v. Leach (1765) 97 ER 1075, Lord Mansfield attacked the discretion that a general warrant devolved to those executing it, stating: "It is not fit, that the receiving or judging of the information should be left to the discretion of the officer. The magistrate ought to judge." A resulting bedrock principle of the warrant system is the need to identify a specific individual or property. The draft IP Bill overturns that principle.

76. Thematic warrants also appear to violate the ECHR. In Zakharov v Russia, the Grand Chamber discussed a number of factors it considers in determining whether "authorisation procedures are capable of ensuring that secret surveillance is not ordered haphazardly, irregularly or without due and proper consideration." It reiterated the principle, expressed in a line of prior cases, that the interception authorisation "must clearly identify a specific person to be placed under surveillance or a single set of premises."[1172]

77. To be clear, communications or equipment *within* the United Kingdom may be intercepted or interfered with under a thematic warrant. These are bulk powers being used against people within the UK.

78. Recommendations

    1. Clause 13

        1. Subsection 13(1)(a) – delete "organisation" and replace with "persons"

1169 The Rt Hon Sir Mark Waller, *Report of the Intelligence Services Commissioner for 2014* (25 June 2015), at pages 18-19, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/437995/50100_HC_225_Intel_Services_Commissioner_accessible.pdf.

1170 Ibid. at page 18.

1171 As Privacy International argued in our submission to the Joint Committee on Human Rights, such warrants are the equivalent of the long prohibited general warrants, and as such should not be allowed. See Privacy International and Open Rights Group's Submission to the Joint Committee on Human Rights on the Draft Investigatory Powers Bill, submitted 7 December 2015, at para. 46, available at http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/human-rights-committee/legislative-scrutiny-draft-investigatory-powers-bill/written/25654.pdf

1172 Zakharov v Russian Federation, [GC], No. 47142/06, 4 December 2015, paras. 259-267.

2. Delete subsection 13(2)

2. Clause 83

1. Subsection 83(a) – delete "organisation" and replace with "persons"

2. Delete subsections 83(b), 83(c), 83(e), 83(f), and 83(g)

79. Questions

1. Would clauses 13(2)(c) and 83 (g), which permit warrants relating to the "testing, maintenance or development" of capabilities for interception or equipment interference, allow security researchers or others who are not a threat to national security or suspected of a serious crime to be the subject of interception or equipment interference?

2. How broadly is "operation" defined? Might "preventing terrorism" be an operation? Might "stopping ISIS" be an operation?

3. If thematic warrants are to be permitted, how will they be regulated to address the concerns raised by the Interception of Communications Commissioner and the Intelligence Services Commissioner?

80. Clause 188: National Security Notices - The extent of the powers contained with clause 188 on National Security Notices is far from clear. Our understanding is that it replaces the powers previously enshrined in the overly broad section 94 of the Telecommunications Act 1984. Some of those powers have purportedly now been made explicit in Part 6, Chapter 2 on bulk acquisition. Clause 188 presumably preserves the rest of them.

81. While clause 188 is somewhat more narrowly drawn than section 94, it still allows the Secretary of State to require a telecommunications operator to take "such specified steps" as she considers "necessary in the interests of national security." Section 94, in contrast, allowed the Secretary of State to make "directions of a general character . . . in the interests of national security." The fact that this old language purportedly permitted the bulk acquisition of communications data from service providers (now in Part 6, Chapter 2) raises serious questions as to what new form of surveillance, that we have not yet considered, might be permitted under clause 188.

82. Further, clause 188(4) states that the "main purpose" of a national security notice cannot be to "do something for which a warrant or authorisation is required under" the IP Bill. Does that mean a national security notice could replace a warrant or authorisation if that's the notice's subsidiary purpose? If so, that would again completely undermine effective judicial authorisation, among many other safeguards.

83. The Explanatory Notes clarify that "[i]n any circumstance where a notice would involve the acquisition of communications or data a warrant or authorization from

the relevant part of this Act would always be required in parallel."[1173] This is a stronger statement than the language in clause 188(4). If the Explanatory Note is correct, then the language of clause 188(4) should be amended to say as much.

84. Recommendations

    1. Clause 188(4)

        1. Delete: "the main purpose of which is"

        2. Amend to read: "But a national security notice may not require the taking of any steps to do something for which a warrant or authorisation is required under this Act. In any circumstance where a notice would involve the acquisition of communications or data a warrant or authorisation from the relevant part of this Act would always be required in parallel."

85. Questions

    1. Given that the language of clause 188 (National Security Notices) remains similar to section 94 of the Telecommunications Act 1984, what would prevent a major expansion of surveillance powers under clause 188, akin to the use of section 94 to acquire bulk communications data?

86. Judicial review - A major topic of the oral evidence presented to the Committee has been the parameters of the "judicial review" standard. This substantial debate demonstrates its meaning is far from clear. For that reason, if the intent is that the Judicial Commissioners shall have the power to fully and completely assess whether a warrant is necessary and proportionate, then any reference to a "judicial review" standard should be removed from the judicial authorisation provisions of the draft IP Bill.

87. Recommendations[1174]

    1. Clause 19

        1. Subsection 19(1): delete "review the person's conclusions as to the following matters" and replace with "determine"

        2. Delete subsection 19(2)

    2. Clause 90

        1. Subsection 90(1): delete "review the person's conclusions as to the following matters" and replace with "determine"

        2. Delete subsection 90(2)

    3. Clause 109

1173 Explanatory Notes, para. 429.

1174 These recommendations are intended to address only the judicial review standard. Throughout this submission we make other criticisms of the judicial authorisation process and bulk powers, for instance, which may necessitate other edits to the clauses referenced here.

1. Subsection 109(1): delete "review the Secretary of State's conclusions as to the following matters" and replace with "determine"

2. Delete subsection 109(2)

4. Clause 123

    1. Subsection 123(1): delete "review the Secretary of State's conclusions as to the following matters" and replace with "determine"

    2. Delete subsection 123(2)

5. Clause 138

    1. Subsection 138(1): delete "review the Secretary of State's conclusions on the following matters" and replace with "determine"

    2. Delete subsection 138(2)

6. Clause 155

    1. Subsection 155(1): delete "review the Secretary of State's conclusions on the following matters" and replace with "determine"

    2. Delete subsection 155(2)

88. Lack of an "examination" warrant for Bulk Personal Datasets (BPD) (Part 7) - Another confusing inconsistency in the Bill is the lack of a "targeted examination warrant" for information obtained through the collection of bulk personal datasets (Part 7).

89. An examination warrant is necessary when material intercepted via bulk interception (Clause 119) or obtained under bulk equipment interference (Clause 147) is to be searched using criteria that is "referable to an individual known to be in the British Islands."

90. But BPDs, which will also contain content referable to individuals in the British Islands,[1175] can be accessed without targeted examination warrants.[1176] The only protection provided is that the original warrant authorizing the acquisition of the BPD must also specify the "operational purposes" for which the data can be examined (Clauses 153(4) & 153(5), and Clauses 154(7) & 154(8)). Those operational purposes, however, can be extremely broad and are elsewhere in the Bill permitted to be "general purposes" (see, for example, Clause 140(5)).

91. Questions

    1. Why isn't an examination warrant required when Bulk Personal Datasets are searched using criteria that is "referable to an individual known to be in the

1175 The definition of "personal data" within the Data Protection Act 1998 includes information that will likely fall in the definition of "content" as provided in Clause 193(6) of the IP Bill.

1176 As we note elsewhere in this submission, we believe providing protections only to those in the British Islands is discriminatory, but if such protections are to exist they should at least be consistently applied across the IP Bill. We also have serious concerns about the collection of bulk personal datasets in the first instance, much less their examination.

British Islands"?

Is the legal framework such that CSPs (especially those based abroad) will be persuaded to comply?

92. While the CSPs are best positioned to answer this question, we note two important considerations.

93. First, by their nature many CSPs have an international presence. As such, they potentially can be subject to conflicting legal obligations imposed by multiple states – from the US and the UK, to Russia and China. How those conflicts should be resolved is the subject of significant ongoing discussion.[1177] By including extraterritorial enforcement provisions in the draft IP Bill, the UK Government is sending a message to the world that any government is justified in reaching outside its borders to impose its will on services used by that government's citizens. The UK needs to think very carefully before setting this troubling precedent.

94. Second, in his report, David Anderson noted that certain US service providers might be more likely to comply with requests from the UK if they were authorised by a judge.[1178] If US service providers might be re-assured by a UK system that includes US-like judicial authorisation, they will not be re-assured by this Bill. As we explain in more detail below, the judicial authorisation regime proposed in the draft IP Bill bears little resemblance to the US system.

Are concerns around accessing journalists', legally privileged and MPs' communications sufficiently addressed?

95. In this response Privacy International focuses on protections for journalists and legal privilege. However, we also note that the IP Bill contains no protection for MPs or members of sensitive professions, such as journalists, lawyers and others, in the context of bulk warrants.

96. Journalists - Clause 61 requires that a Judicial Commissioner authorise the acquisition of communications data for the purposes of identifying or confirming a source of journalistic information. Privacy International has some concerns about this provision.

97. First, Clause 61(1) (a) excludes intelligence services. This should be removed, as protections for journalists should apply to both law enforcement and the security services. No operational case has been made for this distinction.

98. Second, where a journalistic source is to be identified, the standard is higher than the ordinary necessary and proportionate test.[1179] Clause 61 does not meet this stricter standard. While there is some mention of its development in the Codes of Practice, it would be of much greater benefit for the clarity of the protections that these

1177 See, for instance, the Internet & Jurisdiction Project, available at http://www.internetjurisdiction.net/.

1178 David Anderson, *A Question of Trust: Report of the Investigatory Powers Review* (June 2015), at para. 11.19, available at https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf.

1179 See David Anderson report, A question of Trust, paragraph 5.49.

standards be placed into the bill proper and not into secondary legislation.

99. Third, a source is narrowly defined in Clause 61(7) as "an individual who provides material intending the recipient to use it for the purposes of journalism or knowing that it is so likely to be used." In contrast, the Recommendation No. R (2000) 7 from the Council of Europe Committee of Ministers defines a source as "any person who provides information to a journalist".[1180] No intent is required in the Council of Europe definition of a source, and so should not be included in the IP Bill.

100. Finally, judicial authorisation need only be sought if communications data is being obtained for the "purpose" of identifying or confirming a source (Clause 61(1)(a)). This suggests that if source is identified incidentally, no authorisation would be needed. This appears to be a rather broad loophole that, in addition to the lack of protections for journalists and sources in the bulk context, may significantly undermine what protections there are in the IP Bill.

101. Recommendation

    1. Clause 61

        1. Subsection 1(a) delete "(other than an intelligence service)".

102. Questions

    1. How would a test as to whether a person had provided material with the intention for it to be used, or knowledge that information is likely to be used for the purposes of journalism work in practice?

    2. How would the incidental identification of a journalistic source be treated under the IP Bill?

103. Legal Privilege - The IP Bill fails, as RIPA did, to expressly protect legal professional privilege. While Schedule 6 of the IP Bill notes that Codes of Practice will be issued in respect of protections for communications data relating to a member of a profession which would regularly hold legally privileged or relevant confidential information, no further explanation of those protections are included.

104. In the interests of clarity, these protections should be laid down in primary legislation. They protections should apply to both content and communications data, and all forms of surveillance including interception, hacking, or obtaining targeted data from providers. A judge must approve any request to interfere with the privilege.

105. Recommendation:

    1. Make explicit recognition of legal professional privilege in the text of the IP Bill.

106. Question

1180 Recommendation No. R (2000) 7 of the Committee of Ministers to Member States on the Right of Journalists not to disclosure their sources of information, http://www.coe.int/t/dghl/standardsetting/media/doc/cm/rec(2000)007&expmem_EN.asp

1. Why is there no explicit recognition of legal professional privilege in the Bill?

Are the powers sought workable and carefully defined?

107. While we recognise it is a difficult task, carefully defining the powers in the IP Bill is essential to preventing arbitrary and unlawful surveillance. Unfortunately, the current draft of the Bill contains a significant number of provisions that could benefit from more clarity and careful definition, which will also assist in the determination of whether the powers are workable.

Are the technological definitions accurate and meaningful (e.g. content vs communications data, internet connection records etc.)?

108. The technological definitions in the IP Bill raise a number of concerns. In answering this question we focus on the definitions we think are most problematic, including those for: interception; communications data; related communications data; content; telecommunications system, operator, etc. We address ICRs separately in response to the specific questions asked in the "Data Retention" section.
109. Interception (Clause 3) - We are concerned that the definition of interception does not accurately reflect the technical reality of how communications can and will be intercepted and processed.
110. Recently, the Government has advanced the argument that an interference with privacy only occurs when data is examined, or "read", by a person as opposed to a machine. We disagree with this position, as ECHR case law makes clear that the interference with privacy occurs at the time of the interception regardless of whether the data is ever "read" by a person.[1181]
111. The IP Bill, however, defines an interception as an act the effect of which is to "make some or all of the content of the communication available, at a relevant time, to a person who is not the sender or intended recipient of the communication." We question this reliance on making content available to a "person."
112. Surveillance can be undertaken entirely by systems, which can both collect the data and analyse it without the participation of a person. Indeed, we can imagine a scenario in which a surveillance system could analyse the content of a communication in real-time, delete any collected content in real-time, and feed the results of the analysis into an automated profile. At no point in such a scenario would a "person" be involved. Yet the scenario should most certainly be classified as an interception. The definition of interception in the IP Bill should not be construed, therefore, as failing to encompass situations in which a person, perhaps by design, never reads the content of an intercepted communication.
113. Communications Data (Clause 193(5)) – We have long had concerns about the definitions of communications data. We would like to remind the Committee that during the RIPA parliamentary debates there were extensive and detailed discussions around metadata that led to changes. Yet since 2000 the definitions have remained relatively stable, even as communications metadata has dramatically grown in scope

[1181] See e.g. Amann v Switzerland [GC] ECHR 2000-II at §69 ("The Court reiterates that the storing by a public authority of information relating to an individual's private life amounts to an interference within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding.")

and volume, and parliamentary committees have repeatedly noted concerns around the increased sensitivity of metadata. Nonetheless, the only noted change in the definition in the IP Bill is the creation of a new form of metadata for capture, the ICR.

114. In the IP Bill the definition of communications data relies on the definitions of "entity data" (data about a person or thing) and "events data" (data about activities). Communications data is entity or events data that is or may be in possession by a telecommunications operator or available directly from a telecommunication system, but does not include content.
115. The definitions of entity and events data are too vague and fail to take into account the distinctions that may arise in the types of data generated by modern technology. For instance, data about a phone call over landline (e.g. two BT numbers shared a connection for 13 minutes) is vastly different than each 'event' within a chat session (e.g. two subscribers at locations X and Y interacted 97 times over a 13 minute period — sometimes with longer gaps and larger messages, other times with fast messaging indicating agreement or disagreement).
116. Accordingly, the definition of communications data in clause 193(5) is also too vague, but not only because of its reliance on the definitions of entities and events. We also do not understand how communications data may be "comprised in" a communication, but not be content. We are concerned that this would give rise to a situation where there is interception of content in order to reveal communications data. Further, we believe the reference in clause 193(5) to data that is "for the purposes of a telecommunication system" is too broad, and that this should be limited to "for the purposes of a telecommunication system to deliver the communication".
117. Related Communications Data (Clause 3(7)): The bill creates a new version of the definition of 'related communications data' in clause 12(6). This is data collected through interception that relates to the communication, or is comprised in, included as part of, attached to or logically associated with the communication; or it is data that is separable from content that would not reveal the meaning of the communication. If content is defined based on the conveyance of meaning, it is unknown to us how 'related communications data' could be part of content in the first place. The Home Office needs to be clearer on how these definitions interact with the technical specifications of communications. For instance, intercepting at an ISP on port 25 will give access to a communication (e.g. an email) but the "content" (email body) will include the communications data of the email (email headers).
118. Content (Clause 193(6)): The definition of content hinges on the 'meaning of the communication'. We believe greater clarity is required on the constitution of a communication, as applied to all forms of modern and emerging methods of communications. In particular, it is not clear to us, whether an entire communication or just some portion of the communication involves meaning. For instance, an intercepted email does not necessarily fall entirely within "content," but rather only the portion that conveys the meaning, whereas the rest of the email could be defined as communications data or related communications data.
119. The content definition also includes two exceptions. The first, in 193(6a), excludes from content "web browsing" information. We are confused as to why a "future proofed" legislation has such a highly specific reference to web browsing. Is web

browsing only meant to encompass internet connections created when “browsing” through a “browser”, and not through an App on a mobile or tablet device? That is, is it non-content when someone is browsing on BBC or Al Jazeera, but it is content when someone uses the BBC or Al Jazeera News apps for Android or iOS?

120. The second exception, in 193(6b), excludes from the definition of content any 'meaning' arising from the fact of the communication. The very ways in which we communicate today reveals the content of our interactions. Even how our devices interact includes an indication of sensitive personal activity. The meaning of a communication can sometimes be discerned just from the fact that an interaction took place. For instance, the meaning of a call to an abuse help-line or browsing the website of a support group is relatively clear. Yet 6(b) explicitly excludes this from content, and thereby ensures weak protections and safeguards for its access. This exception is an admission by the government that they view communications data as sometimes quite revelatory but they nonetheless insist that authorities must be able to access this ‘meaning’ with fewer safeguards.
121. Telecommunications System, Operator, Service etc (Clause 193): The definitions of telecommunications operators, services and systems lack sufficient exclusivity. The ambiguity in the terms means that a given communications provider could fit into different definitions simultaneously. An Internet Service Provider like Zen Internet or AAISP could be a telecommunication system (as they have wires and cables), telecommunication service (as they deliver services), and telecommunications operator. Equally, Facebook could be any of these because the definition of system is based on “facilitation” of the communication. This ambiguity might reflect the intention that the Bill be as technology neutral as possible. But it gives too much discretion to the Secretary of State in deciding when a service provider fits in each definition. This creates regulatory uncertainty.

Does the draft Bill adequately explain the types of activity that could be undertaken under these powers?

122. No. As noted above, the definitions at the heart of some of the powers, like interception, are unclear. Equipment interference is also not well delineated. For instance, how equipment might be interfered with – the method that could be used to obtain the communications, private information and equipment data listed in clause 81 – is never described. This leaves us guessing at what types of activities might be carried out, especially under a power as seemingly broad as equipment interference. Similarly, bulk personal datasets are so broadly defined that it is not clear what limits, if any, there are on the data that might be obtained from public or private sources.

123. Furthermore, many of the powers allow for the taking of “necessary" steps that are not explicitly authorised in the warrant. For example, clause 12(5)(a)(i) permits conduct that is necessary to carry out what is expressly authorised in the warrant, but does not specify or in any way limit that conduct.

124. The Bill also places a number of open-ended obligations on other parties to assist, facilitate or implement many of the powers (such as Clauses 29 and 31). Again, little or no detail is given regarding the assistance that may be required - or more importantly what activities are prohibited. Only clause 189 provides some examples,

including the removal of electronic protection, which are more troubling than reassuring.

125. Finally, as noted in paragraphs 80 to 85 above, clause 188 appears to be a catch-all provision that if not narrowed could permit activities that we cannot even imagine at this time.

126. Questions

1. What activities fall within the definitions of interception and equipment interference? What is prohibited?

2. What types of bulk personal datasets may be collected from public and private sources?

3. What may telecommunications services and operators be asked to do in order to assist in carrying out a warrant for any of the enumerated powers?

Is the wording of the powers sustainable in the light of rapidly evolving technologies and user behaviours?

127. As technology continues to evolve into every facet of life and individuals adapt their behaviours to engage with these changes, it is crucial that legislation keeps pace with these advances. The IP Bill in its current form offers little concrete detail of how the provisions will be implemented (as described in the previous section). The vagueness of some of the wording runs the risk that surveillance powers will be used to conduct activities not currently envisioned. The non-technical language used to describe some of the powers threatens to creep into the realm of fantasy with its lack of technological underpinning. In this regard, it is very difficult to assess how the IP Bill will apply to current technology, let alone new technologies.

128. Rather than using ambiguous terminology, it would be preferable to use more specific technology-oriented language and apply a review process to the legislation on a regular basis. This would allow for greater specificity in the language of the Bill, while also allowing amendments at reasonably regular intervals to accommodate changes in user behaviour and the technological climate.

Overall is the Bill future-proofed as it stands?

129. Technology changes rapidly. Yet technology-neutral legislation that attempts to accommodate that change can also pose serious risks to privacy and security as technological development and innovation dramatically transform the scope of prior, vaguely worded powers.

130. We are often not equipped to understand how these powers will apply today, much less to likely technologies of tomorrow. Parliamentary debates around RIPA did not anticipate popular webmail providers based in foreign jurisdictions, extensive location data collected by devices and networks, and broad-scale interception capabilities. All these technologies appeared shortly after RIPA and fuelled surveillance capabilities for at least the next ten years.

131. We would prefer surveillance legislation that errs on the side of being too specific. This way Parliament can understand how it applies and assess the costs, benefits, and implications.

132. When the Joint Committee reviewed the draft Communications Data Bill, the Committee found that the order-making powers given to the Secretary of State were too great. This was, the Home Office argued at the time, essential to future-proofing the legislation. That is, as technologies changed, the Secretary of State did not want to seek new authorisation from Parliament to apply the powers to each new technology.

133. We believe that the IP Bill repeats this mistake. It contains vague and ill-defined terms, and places obligations on telecommunication operators and others, in the UK and abroad, to provide and, when necessary, generate data, to retain data, and to enable interception and interference, in targeted and bulk manners. The concern is that these demands placed today will shape and limit the kinds of services developed tomorrow.

134. One possible direction of innovation is the Internet of Things. Soon many more devices, ranging from refrigerators to thermostats, cars to toasters, will be recording and communicating information about us, and not necessarily to us. These devices can be interfered with, their communications intercepted and their data shared. They may even be co-opted to gather more information. We must therefore not debate the IP Bill as though it applies only to mobile phones and laptops. We may soon be surrounded by and wearing technologies that can be used by governments and others, both in the UK and abroad, to place us under surveillance.

135. As a small reminder of history, within weeks of RIPA being given Royal Assent, the Home Office was actively pursuing new powers of data retention. A year and a half later, voluntary data retention was law. Before long, mass collection and interception exercises were in place. Six years later the Home Office was developing formal policy to support mass collection of communications data of over the top services. This current draft Bill not the last piece of legislation for new powers that will be introduced by the Home Office in the foreseeable future.

136. <u>Recommendation</u>

    1. Parliament should debate the extent of powers it is granting to authorities, and how these powers are being used, on a regular basis.

137. <u>Questions</u>

    1. How will Parliamentarians be informed about the nature of changing telecommunications technologies and their impact on the law?

    2. What assessments have been made to understand how these powers are used with respect to new and emerging technologies like the Internet of Things?

Are the powers sought sufficiently supervised?

138. While some progress is made in the IP Bill through the introduction of the Judicial

Commissioner, it nonetheless leaves significant powers in the hands of the Secretary of State with no, or insufficient supervision. Like the Draft Communications Data Bill, much of the IP Bill requires secondary actions, whether regulation or subsequent actions by the Secretary of State.

139. In our review of the various capabilities granted but not specifically established in the Bill, Secretary of State may, inter alia:

    1. choose to enforce a duty upon telecommunications operators through civil proceedings (clause 31(8));

    2. establish, maintain and operate a filter and related arrangements (Clause 51), though in consultation with the Investigatory Powers Commissioner (IPC) as to the principles of the basis of the arrangements; and transfer these functions to any other public authority (Clause 67);

    3. modify, by regulations, the relevant public authorities and designated senior officers and the authorities of those departments and agencies in Schedule 4 (Clause 55), in consultation with the IPC and the public authority;

    4. require, by notice, a telecommunications operator to retain relevant communications data (Clause 71(1)), by giving, or publishing, it in such manner as he or she considers appropriate (Clause 71(6)); and

    5. require, by notice, a telecommunications operator to take any further steps that the Secretary of State considers necessary in the interest of national security, that may in particular require the operator to carry out any conduct to facilitate anything done by an intelligence service or dealing with an emergency, or provide services or facilities to do so (Clause 188).

140. One of the key concerns is the maintenance of technical capability provision (Clause 189). The Secretary of State can require, inter alia, the provision of facilities or services of a specified description and the removal of electronic protection applied by a relevant operator. Though the Secretary of State must consult with certain people, including the Technical Advisory Board and persons likely to be subject to the obligations, such consultation is only a weak check on the Secretary of State's authority.

141. Furthermore, we question the extent to which modifications and extensions can be made to warrants without adequate supervision or judicial authorisation (Clauses 96, 97, 114, 128, 143, 162.) For example, names or descriptions can be added to targeted interception warrants without authorisation or other involvement of Judicial Commissioners (Clause 26).

142. We are also concerned that the IPC can approve warrants that were rejected by Judicial Commissioners without any clear follow-up process of review.

143. <u>Question:</u>

    1. What powers will the Technical Advisory Board have to demand supervision over specific capabilities and how they are deployed?

2. If the above powers mentioned in this section are to remain in the IP Bill (and we argue a number of them should not), why couldn't the powers be transferred from the Secretary of State to the Judicial Commissioners?

Is the authorisation process appropriate?

144. No. Privacy International submits that the authorisation process articulated in the draft IP Bill is not appropriate. Authorisation must entail fully independent judicial authorisation, where judges have unfettered discretion to determine if a warrant sought by the executive is necessary and proportionate. The draft Bill, by contrast, preserves the power of the Secretary of State to issue warrants. While it permits Judicial Commissioners to "approve" this decision, it places significant limitations on the scrutiny they can exercise in reviewing the warrant (see in particular Clauses 19-21, 90, 109, 123, 138, 155). And in some instances, it does not require any form of judicial approval at all (see Clauses 26, 46, 71).
145. In deciding whether to approve the issuance of a warrant, a Judicial Commissioner is to apply the "judicial review" standard. The precise contours of this standard are subject to some debate and we recognise that multiple interpretations have been presented to the Committee. Our understanding, which is also articulated by Liberty, is that this standard constrains review to procedural propriety and prohibits examination of the merits.[1182] If the intent is for Judicial Commissioners to have unrestricted authority to assess whether a warrant is necessary and proportionate, then any reference to a "judicial review" standard should be stripped from the judicial authorisation provisions of the draft IP Bill. The fix is simple – just delete sub-section (2) from each of the clauses describing "Approval of warrants by Judicial Commissioners" and slightly reword sub-section (1), as we propose above in paragraph 87.
146. Judicial authorisation, even in the weak form expressed in the draft IP Bill, is not required for the Government to acquire communications data, issue data retention notices or modify interception warrants, all of which interfere with the right to privacy. In our prior submission to the Joint Committee on Human Rights, we noted that the lack of judicial authorisation for such powers might fall short of requirements under international human rights law.[1183]
147. We also have serious concerns about whether any authorisation process – judicial or not – is workable in the bulk context. The sheer breadth of a bulk warrant inherently frustrates substantive review of its necessity and proportionality. As we also submitted to the Joint Committee on Human Rights, bulk warrants need not "specify or target the communications, data or equipment of a particular person, premises or even an organisation."[1184] They need only "state the operational purposes for which

1182 The Courts and Tribunals Judiciary has also adopted this interpretation on their website:

> [J]udicial reviews are a challenge to the way in which a decision has been made, rather than the rights and wrongs of the conclusion reached. It is not really concerned with the conclusions of that process and whether those were "right", as long as the right procedures have been followed. The court will not substitute what it thinks is the "correct" decision.

Courts and Tribunals Judiciary, "Judicial review", https://www.judiciary.gov.uk/you-and-the-judiciary/judicial-review/.

1183 Joint Committee on Human Rights Submission, paras. 51-56.

1184 *Id*. at para. 20.

data need to be obtained, and the IP Bill expressly notes that these can be 'general purposes'" (see Clauses 111(4), 125(4), 140(5)). This lack of specificity – *i.e.* the absence of any assessment of suspicion – is intrinsically disproportionate and runs afoul of explicit guidance from the ECtHR.[1185]

148. It may be useful to look at the American context where judicial authorisation is the norm. Under the US Wiretap Act, the Attorney General "may authorize an application to a Federal judge for . . . an order . . . approving the interception of wire or oral communications".[1186] The judge may only approve a wiretap order if he or she "determines on the basis of the facts submitted by the applicant" that, *inter alia*: (a) there is probable clause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in the Act; (b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception; (c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous.[1187]
149. In the US, the notion of independent judicial authorisation of warrants is sacrosanct and for good reason. In the words of the US Supreme Court in the landmark "Keith" case:

> "Inherent in the concept of a warrant is its issuance by a "neutral and detached magistrate." . . . The [Constitution] does not contemplate the executive officers of Government as neutral and disinterested magistrates. Their duty and responsibility are to enforce the laws, to investigate, and to prosecute. But those charged with this investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means in pursing their tasks. The historical judgment . . . is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech."[1188]

150. Importantly, the Court continued that this risk is particularly acute in the national security context "because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent."[1189]
151. The US is hardly unique in this respect. In fact, the passage of the draft IP Bill with the current authorisation process would continue to make the UK an outlier among other democratic countries and the only state in the Five Eyes Alliance (which also includes the US, Australia, Canada and New Zealand) that does not vest the power to approve surveillance activities in the judiciary.[1190] It would also fly in the face of Anderson's explicit recommendation that "the warrant-issuing powers currently vested in the Secretary of State . . . be exercised only by Judicial Commissioners".[1191] For all of

---

1185 *Id*. at paras. 21-22 (discussing Gillan and Quinton v United Kingdom and S and Marper v. United Kingdom).

1186 18 U.S.C. §§ 2510-2522.

1187 *Id*. at § 2518. These requirements are enshrined in Rule 41 of the Federal Rules of Criminal Procedure with respect to "Search and Seizure" more generally.

1188 United States v. United States District Court for the Eastern District of Michigan ("the Keith case"), 407 U.S. 297, 316-17 (1972). In the Keith case, the Supreme Court unanimously held that the government was obligated to obtain a warrant before conducting electronic surveillance even for the purposes of domestic threats to national security.

1189 *Id*. at 320.

1190 Liberty, "Safe and Sound", https://www.liberty-human-rights.org.uk/campaigning/safe-and-sound.

1191 Anderson Report, para. 14.95(b); *see also id*. at Recommendation 22 ("Specific interception warrants, combined warrants, bulk interception warrants and bulk communications data warrants should be issued and renewed only on

these reasons, we believe the authorisation process currently proposed in the draft IP Bill is inappropriate.

152. Recommendation:

1. Vest the power to issue warrants in Judicial Commissioners or, in the alternative, remove the "judicial review" standard in the approval clauses as described in paragraph 87 above.

2. Ensure prior judicial authorisation for the acquisition of communications data and the modification of warrants.

153. Question

1. In the context of bulk powers, how can necessity and proportionality be judged in the authorization process?

Will the oversight bodies be able adequately to scrutinise their operation?

154. Clauses 180 and 181 add to RIPA's provisions on the role of the Investigatory Powers Tribunal (IPT). The IPT has operated as a secret court and "sits outside the regular structures of British justice"[1192]. Notably, both the Anderson and RUSI reviews called for an overhaul of the IPT.[1193] The draft Bill does not address the flaws of the IPT, although clause 180 does encouragingly allow an appeal to be made to a UK court. Below, we propose some specific reforms of the IPT and this new right of appeal in response to the question, "Are the new arrangements for the Investigatory Powers Tribunal including the possibility of appeal adequate or are further changes necessary?"

155. The establishment of a new IP Commissioner, which would replace the Interception of Communications Commissioner, the Chief Surveillance Commissioner, and the Intelligence Services Commissioner, is a welcome step.

156. Clause 167(1) states that the Prime Minister will appoint the IP Commissioner. This is inappropriate as it means that the IP Commissioner's role will not be properly independent from the Executive. The Judicial Appointments Commission (JAC) should appoint the IP Commissioner and the related Judicial Commissioner, which will give both the public and Parliament greater confidence that this vital role is independent.

157. Ensuring an appropriate level of resourcing for the IP Commission will be crucial in enabling the public and Parliament to ensure surveillance powers are properly used. We understand that the current proposal is to appoint one IP Commissioner and only seven Judicial Commissioners. In order to provide an appropriate level of oversight,

---

the authority of a Judicial Commissioner."). The RUSI Report recommended a modified regime whereby warrants "sought for a purpose relating to the detection or prevention of serious and organised crime . . . should always be be authorised by a judicial commissioner" whereas warrants "sought for purposes relating to national security . . . be authorised by the secretary of state subject to judicial review by a judicial commissioner." RUSI Report, Recommendation 10.

1192 Murphy, C. C. & Simonsen, N. (5 November 2015) Interception, Authorisation and Redress in the Draft Investigatory Powers Bill, *UK Human Rights Blog* [Online], available at http://ukhumanrightsblog.com/2015/11/05/interception-authorisation-and-redress-in-the-draft-investigatory-powers-bill/ [Accessed 15 December 2015]

1193 *See* Anderson Report, paras. 14.103-08; RUSI Report, Recommendations 11-16.

there needs to be a much more substantial body of Judicial Commissioners.

158. While we welcome the three roles that need to be carried out, namely authorisation, inspection, and informing the public and Parliament about "the need for and use of investigatory powers", there will be an irresolvable conflict of interest if the same body both authorises and then also somehow independently reviews those authorisations to ensure they were lawful and carried out properly. In order to engender public trust, oversight of the use of surveillance must be separate from authorisation of surveillance.

159. The draft Bill has very little to say about redress. While Clause 171(1) does state that the new IP Commissioner "must inform a person of any relevant error", Clause 171(2) sets a very high bar, in that both the IP Commissioner and IPT must agree that it is a "serious" error and that it is in the public interest for that person to be informed of the error. What is considered "serious" needs further explanation, and what the public interest test will be is not clearly defined. We suggest deleting both requirements and allowing the IP Commissioner to reveal any error in the interest of transparency and public accountability.

160. In our prior submission to the Joint Committee on Human Rights, we discussed how the draft IP Bill contains a range of provisions that prohibit and, in some cases, criminalise unauthorised disclosure (see Clauses 43-44, 66, 77, 102, 133, 148, and 190).[1194] We noted that these gagging clauses, by prohibiting notification of surveillance measures, might be violative of the ECHR. If individuals are unaware that a public authority has obtained their data, they will not be able to seek redress.

161. <u>Recommendations:</u>

    1. Clause 167 - Subsection 167(1) – delete "Prime Minister" and replace with "Judicial Appointments Commission".

    2. Remove the "serious error" requirement and "public interest" test from Clause 171 and delete clause 171(4).

    3. Add language to provide further detail about how the IPT will be transparent and accountable, as we suggest in paragraph 295.

    4. Soften strict non-disclosure clauses by permitting a public interest defence for unauthorised disclosure and permitting service providers, with limited exception, to notify individuals.

What ability will Parliament and the public have to check and raise concerns about the use of these powers?

162. Privacy International is concerned that surveillance oversight bodies often operate at a disadvantage. For instance, an advanced understanding of technology is required to comprehend analytical capabilities, modern interception capacities, and the security implications of hacking activities. The oversight bodies mentioned in the IP Bill do

1194 Joint Committee on Human Rights Submission, paras. 61-68.

not always have that expertise.

163. Current oversight also relies too heavily on self-reporting by the relevant investigatory agencies. Parliamentary oversight committees and former senior government officials have been surprised by the use of some powers, and many of these powers were only admitted as a side-effect of an investigation and not necessarily through simple reporting, e.g. the use of bulk personal data sets.

164. Within the IP Bill, the IPC will report on a yearly basis to the Prime Minister, and the Prime Minister must publish the report and lay a copy before Parliament (Clause 174(6)). We are concerned that the Prime Minister can exclude from publication any part of a report if, in the opinion of the Prime Minister, the publication would be contrary to the i) public interest, or ii) prejudicial to national security, prevention or detection of serious crime, or the economic well-being of the United Kingdom. While we recognise there will be some legitimate reasons to withhold certain operational information, the presumption should be in favour of transparency. It thus seems highly unlikely that the public interest will weigh in favour of redaction unless there is also a threat to national security or the prevention and detection of serious crime. The language of clause 174(6) could therefore be tightened to allow for more transparency.

165. In order to reduce reliance on whistleblowers, we suggest softening the offence of making an unauthorised disclosure in clauses 43, 66 and 102 as there seems to be little opportunity for any disclosure beyond the mere number of warrants received (see paragraph 160). In particular with regards to clause 102 within equipment interference, there are no authorised disclosures, and this prevents companies from openly discussing how (bulk and targeted) equipment interference warrants may interfere with their service delivery, the implications of the imposition of the warrant, and any steps taken. This further stems the public's ability to understand how the powers are used and will adversely affect global cybersecurity.

166. <u>Recommendation:</u>

1. We believe that the public needs more information on how investigatory powers and capabilities have been developed and used.

167. <u>Questions:</u>

1. How will the Secretary of State and Parliament ensure that the oversight bodies have sufficient independent technological understanding?

2. How will the oversight bodies regularly be made aware of the investigatory capabilities that are being developed and deployed?

3. Why is there no ability of operators and services to notify customers of the receipt of a warrant or other notice if such notification would not interfere with necessary secrecy?

4. Why are transparency reports limited to only the numbers of warrants received?

5. Why does the IPC report to the Prime Minister and not directly to Parliament?

Specific questions

General

To what extent is it necessary for (a) the security and intelligence services and (b) law enforcement to have access to investigatory powers such as those contained in the Draft Investigatory Powers Bill?

168. We respectfully refer the Committee to our responses to the questions:
    1. "Has the case been made, both for the new powers and for the restated and clarified existing powers?" (paragraphs 13-37)
    2. "Are the power compatible with the Human Rights Act and ECHR?" (paragraphs 38-58)
    3. "Is the requirement that they be exercised only when necessary and proportionate fully addressed?" (paragraphs 59-64)
169. In those responses, we articulated why the Government has failed to demonstrate the operational and legal (under the "necessary and proportionate" test) necessity for either the security and intelligence services or law enforcement to have access to the following investigatory powers:
    1. bulk warrants
    2. acquisition of ICRs as part of communications data
    3. data retention
    4. equipment interference
    5. thematic warrants

Are there any additional investigatory powers that security and intelligence services or law enforcement agencies should have which are not included in the draft Bill?

170. While we do not comment on whether the security and intelligence services or law enforcement need any powers that are not already in the IP Bill, we would like to reinforce that any powers that are claimed should be made clear and foreseeable in statute, as is required by the rule of law and so that any interference with privacy will be "in accordance with law". Significant new powers must not be brought about through the reinterpretation of the IP Bill or within Codes of Practice. If a new power is sought which is not reasonably foreseeable within the existing law, it must be authorised through a change to the primary legislation. This will allow a legislative debate about the power, a clear case to be made for their use, and further explanation of how the new power is necessary and proportionate.

171. Unfortunately, the IP Commissioner is not permitted to review "the exercise of any function of a relevant Minister to make or modify subordinate legislation," (Clause 169(4)(a)). If the IP Commissioner is not reviewing such power, who will to ensure it does not result in a significant change to the primary legislation? The answer is currently missing from the draft IP Bill.

172. Questions:

    1. What is the process for any new power or re-interpretation of existing powers to be debated, passed and communicated to the public?

2. How does the IP Bill stop another situation like the one described by Anderson in his review of RIPA and his opening lines of A Question of Trust: "RIPA, obscure since its inception, has been patched up so many times as to make it incomprehensible to all but a tiny band of initiates. A multitude of alternative powers, some of them without statutory safeguards, confuse the picture further. This state of affairs is undemocratic, unnecessary and – in the long run – intolerable"?

Are the new offences proposed in the draft Bill necessary? Are the suggested punishments appropriate?

173. Clause 2 sets out the offence of unlawful interception and clause 6 sets out the penalties. In particular, subsection 6(b) identifies a penalty that "must not exceed £50,000". Privacy International does not have a view of the appropriate monetary penalty, but as this is a serious offence, we do believe that there should be serious commensurate penalties.

174. Clause 8 sets out the offence of unlawfully obtaining communications data. While we agree it is correct that this is an offence, again we do not have a view on what the appropriate punishment should be.

175. As discussed in paragraph 160 the draft IP Bill contains a range of provisions that prohibit and, in some cases, criminalise unauthorised disclosure (see Clauses 43-44, 66, 77, 102, 133, 148, and 190).[1195]

176. Privacy International believes it is inappropriate to ban and make criminal all forms of disclosure. There are some circumstances under which telecommunications operators and services should be able to notify their customers that their personal information has been shared with the state. The current prohibitions are both potentially violative of the ECHR and run counter to the purported aim of the draft Bill to create greater transparency. While it might not be appropriate for all operational details to be published, high-level information should be published about the types of warrants and notices that are being served on telecommunications providers.

177. <u>Recommendations</u>

    1. Soften strict non-disclosure clauses by permitting a public interest defence for unauthorised disclosure and permitting CSPs, with limited exception, to notify individuals.

<u>Interception</u>

Are there sufficient operational justifications for undertaking (a) targeted and (b) bulk interception?

178. We respectfully refer the Committee to our response to the question:
    1. "Has the case been made, both for the new powers and for the restated and clarified existing powers?" (paragraphs 13-37)

1195 Joint Committee on Human Rights Submission, paras. 61-68.

179. In that response, we articulated why the Government has failed to make a compelling operational case for undertaking bulk interception. We also detailed how the Government has similarly failed to make a compelling operational case for expanding targeted interception to include the use of "thematic warrants".

Are the proposed authorisation processes for such interception activities appropriate? Is the proposed process for authorising urgent warrants workable?

180. In terms of whether the proposed authorisation processes for interception activities are appropriate, we respectfully refer the Committee to our response to the question:
    1. "Is the authorisation process appropriate?" (paragraphs 144-153)
181. In that response, we explain why the authorisation process articulated in the draft IP Bill for all proposed powers, including interception activities, is not appropriate. For similar reasons, we also submit that the proposed process for authorising urgent warrants is, in general terms, not workable.
182. The urgent warrant authorisation process is also problematic for three additional reasons. First, the term "urgent" is not defined anywhere in the draft IP Bill and could therefore be interpreted to encompass a wide array of circumstances. By way of comparison, the US Wiretap Act, which regulates the interception of wire and electronic communications, strictly limits "urgent" interception – *i.e.* without prior judicial authorisation – to the following "emergency situations": (i) immediate danger of death or serious physical injury to any person, (ii) conspiratorial activities threatening the national security interest, or (iii) conspiratorial activities characteristic of organized crime.[1196] We urge the Committee to consider defining "urgent" to a similar set of limited and specific circumstances.
183. Second, the urgent warrant authorisation process requires the Secretary of State to inform a Judicial Commissioner that such a warrant has been issued but does not indicate the timeframe in which this notification is to occur (Clauses 20(2), 91(2), 156(2)). As another point of comparison, the US Wiretap Act requires that where an urgent warrant is issued, "an application for an order approving the interception" must be made to a judge "within forty-eight hours after the interception has occurred".[1197] In contrast, the draft IP Bill provides that a Judicial Commissioner has five "working" days to review the issuance of the warrant. Others have argued that five days is too long of a timeframe.[1198] We note here that five "working" days can potentially elongate that timeframe even further. As an example, a warrant issued on Thursday, March 24 2016 would not have to be approved until over one week later, on Monday, 4 April 2016, taking into account weekends and bank holidays. The lack of a specific timeframe for notifying a Judicial Commissioner combined with the long timeframe for review creates the risk that unlawful urgent warrants may, in practice, operate for inappropriately long periods of time before they are struck down.
184. Finally, we note that the urgent warrant authorisation process provides that where a

1196 18 U.S.C. § 2518(7)(a).
1197 *Id*. at § 2518(7)(b).
1198 *See, e.g.*, The Bar Council, "Bar Council comments on Draft Investigatory Powers Bill", 5 Nov. 2015, http://www.barcouncil.org.uk/media-centre/news-and-press-releases/2015/november/bar-council-comments-on-draft-investigatory-powers-bill/ ("As all lawyers know, there is a duty judge available through the Royal Courts of Justice 24 hours a day. There is no reason why such provision could not be made available in cases where investigatory powers are being sought.").

Judicial Commissioner refuses to approve a warrant, he may but is not directed to order that the material obtained under the warrant be destroyed (Clauses 21(3), 92(3), 157(3)). Indeed, he may simply "impose conditions as to the use or retention" of the material. We question why it should ever be permissible for the Government to use or retain material that was unlawfully acquired and therefore urge the Committee to consider requiring destruction of the material in such circumstances.

185. Recommendations:[1199]
    1. Define the term "urgent" as used in Clauses 20, 91 and 156.
    2. Provide a timeframe within which the Secretary of State must inform a Judicial Officer that an urgent warrant has been issued in Clauses 20(2), 91(2) and 157(2).
    3. Provide a shorter timeframe than five "working" days within which a Judicial Commissioner must review the issuance of an urgent warrant.
    4. Change the word "may" to "must" in Clauses 21(3), 92(3) and 157(3). Delete Clauses 21(3)(b), 92(3)(c) and 157(3)(b).

Are the proposed safeguards sufficient for the secure retention of material obtained from interception?

186. Intercepted data is highly sensitive. Large organisations often face problems in securing retained information, particularly valuable information that is to be accessed by many users. In a modern society where physical storage devices have dramatically dropped in price, we are too slowly realising that the limitation on generation, collection, and retention of information involves costs other those associated with mere storage. The various data breaches over the years, including the recent breaches of government agencies and telecommunications companies should give us pause (see paragraph 234 for more details).
187. Even systems designed to detect intrusions and prevent them can themselves be corrupted.[1200] Given their access to data, such systems are an extremely attractive target for malicious third parties.
188. The IP Bill contains no details regarding how information in storage is to be made "secure." At the very least, the Bill should specify the minimum technical requirements for securing retained data, and describe how any breaches will be addressed and revealed to oversight bodies and the public.
189. Recommendations
    1. Include detailed provisions describing how retained data will be secured.
    2. Include a mechanism by which oversight bodies and the public will be informed of breaches.

How well does the current process under Mutual Legal Assistance Treaties (MLATs) work for the acquisition of communications data?

190. Looking at the regime between the UK and the US and taking the example of the UK as the requesting party, the Mutual Legal Assistance (MLA) process to obtain content data currently functions as follows: the UK sends a request for communications content data stored by a US company to the US Department of Justice (DOJ) Office of

[1199] While making these recommendations, we maintain the criticisms of the underlying powers that we make elsewhere in this submission which in some cases might dictate the complete removal of certain referenced clauses.
[1200] See Steve Ragan, "Researcher discloses zero-day vulnerability in FireEye," CSO Online (6 Sept. 2015), available at: http://www.csoonline.com/article/2980937/vulnerabilities/researcher-discloses-zero-day-vulnerability-in-fireeye.html

International Affairs (OIA). OIA works with the UK to ensure the request satisfies US legal standards and then works with a US Attorney to send the request to the District Court. The judge reviews the request and grants it, or sends it back to OIA for further iterations with the requesting country. If granted, the request goes to the company, which sends a response to OIA, which checks the response and in turn sends the response to the UK.[1201]

191. Notably, this process only applies to requests for content data; companies have discretion about how to respond to foreign requests for communications data.

192. The IP Bill currently contains a proposed mutual assistance warrant (Clause 12) through which the UK will provide assistance in intercepting communications where required by an MLAT. Clause 39 provides for a separate authorisation for the interception of communications in accordance with overseas requests. Privacy International is unclear as to how these two clauses interact (Clause 12 and Clause 39) and encourages members of the Committee to seek clarification from the Home Office on this point.

193. When it comes to communications data, the IP Bill provides no specific procedure for the acquisition of such data under an MLAT. Instead, Clause 69 specifically notes that acquisition of communications data power has an extra-territorial application, by noting that an authorisation to obtain communications data may relate to persons or telecommunications providers outside the UK.

194. This provision is of significant concern, particularly in light of the fact communications data authorisations may be issued without judicial approval. We address the problems raised by extraterritorial powers more generally in paragraphs 93 to 94, and in response to the following question.

195. Question:

1. How do the mutual legal assistance warrants described in Clause 12 and Clause 39 interact in connection with an overseas request for interception assistance? Does Clause 39 permit a telecommunications service to respond to an MLAT request even if a warrant is not issued under Clause 12?

What will be the effect of the extra-territorial application of the provisions on communications data in the draft Bill?

196. Clause 69 makes foreign telecommunications operators subject to the UK's power to acquire communications data. While clause 69(4) provides potential exemptions, based on the requirements and restrictions on data acquisition in operators' own countries, placing such obligations on service providers in the first place sets a bad precedent for the rest of the world, as discussed above in paragraphs 93 to 94.

197. Clause 79(2) asks foreign telecommunications providers to retain communications data. Unlike in Clause 69, there is no obligation to "comply", only a "duty to have

1201 Swire, Peter, and Hemmings, Justin. "Re-Engineering the Mutual Legal Assistance Treaty Process." NYU Law and PLSC Conferences. 14 May 2015.

regard to the requirement or restriction" regarding data retention. This puts an ambiguous responsibility on foreign companies. It will also reduce customer trust in these companies, as the customers will not know whether their service provider is complying with retention requests or not. The obligation, whether to comply or to have "regard" should be completely removed from the Bill.

198. Placing extraterritorial obligations on companies can have other negative consequences. For example, Google withdrew their operations from China[1202] based on the Chinese government placing similar obligations on technology companies.

199. As discussed in paragraph 94, foreign companies are more likely to comply with requests if they are authorised by a judge.[1203] It would set a very worrying international precedent if foreign companies were to hand over their customers' data based on the request of a UK politician. Should UK companies ever be required to hand over their customers' data based on a warrant approved by the Chinese government?

200. The recent case of WhatsApp being shut down across Brazil, because they were unable to comply with an order to place wiretap requests on some customer accounts, highlights the problem of placing unreasonable obligations on a company to provide customers' personal data to a foreign government.[1204]

201. Recommendations

1. Delete clauses 69 and 79

Communications Data

Are the definitions of content and communications data (including the distinction between 'entities' and 'events') sufficiently clear and practical for the purposes of accessing such data?

202. As we state above, we have difficulty understanding and parsing these definitions. Please see our response to the question, "Are the technological definitions accurate and meaningful (e.g. content vs communications data, ICRs etc.)?"

Does the draft Bill allow the appropriate organisations, and people within those organisations, access to communications data?

203. Schedule 4 of the draft Bill lists the public authorities that will be able to access communications data. However, Clause 55(2a) enables the Secretary of State to add to or remove public authorities from this list. The circumstances under which changes will be made needs to be set out, as should the mechanisms for consulting and notifying the public of any changes. As currently drafted, the public will not be

1202 Criticism and regret in China over Google, *BBC News* [Online] http://news.bbc.co.uk/1/hi/world/asia-pacific/8583006.stme

1203 David Anderson, *A Question of Trust: Report of the Investigatory Powers Review* (June 2015), at para. 11.19, available at https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf

1204 Goel, V, and Sreeharsha, V. Brazil Restores WhatsApp Service After Brief Blockade Over Wiretap Request, *New York Times* [Online], Available from http://www.nytimes.com/2015/12/18/world/americas/brazil-whatsapp-facebook.html?ref=americas&_r=0

provided with any clarity or assurance of which public authorities will be able to collect their communication data.

204. It is inappropriate that such a long list of public authorities has access to individuals' communications data and for such broad purposes. This is a problem in its own right, but it also further reinforces the need for judicial authorization, which we discuss in more detail below in response to the question, "Is the authorisation process for accessing communications data appropriate?"

205. Furthermore, Clause 60(1) of the draft Bill sets out the requirement for a designated senior officer to consult a 'single point of contact' (SPOC) before granting an authorisation to obtain communications data. This is often cited as important safeguard on communications data requests.

206. The SPOC does not have any authority over the requests, however. Instead there is only a requirement to "consult" the SPOC, which falls short of even being a rubber stamp. The SPOC should have greater involvement in approving requests.

207. But the SPOC should not have overall responsibility for approving requests for communications data. Given how revealing communications data is about an individual, access to it must be subject to judicial authorisation.

208. Our concerns about the number of people who can access communications data are compounded by Clause 46(7), which sets out an overly broad range of purposes for which communications data may be obtained. Clause 46(7b) in particular, which is about preventing or detecting crime or disorder, is too broad and enables intrusive 'fishing expeditions'. The provision should be amended to 'serious crime'.

209. Recommendations:

1. Require judicial authorisation for obtaining communications data, and give the SPOC a more substantial role in the authorization process.

2. Significantly limit the purposes for which communications data can be obtained.

Are there sufficient operational justifications for accessing communications data in bulk?

210. We respectfully refer the Committee to our response to the question:

1. "Has the case been made, both for the new powers and for the restated and clarified existing powers?" (see paragraphs 12-37).

211. In that response, we articulated why the Government has failed to make a compelling operational case for any of its bulk powers, including for accessing communications data in bulk.

Is the authorisation process for accessing communications data appropriate?

212. No. There is no prior judicial authorisation (with the only exceptions for local authorities under Clause 59; and if the authorisation is required in relation to obtaining communications data for the purpose of identifying or confirming a source

of journalistic information, Clause 61.) Ordering the disclosure of communications data only requires authorisation by a designated senior officer of the public authority undertaking the collection. The limited safeguard of requiring the authorisation not be granted by an officer involved in the investigation or operation is undermined by the broad set of circumstances under which such requirement can be overridden (Clause 47).

213. The collection and use of communications data interferes with the right to privacy.[1205] In fact, it is not disputed that communications data allow "very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained.[1206] As such authorisation for the collection and use of such data needs to fulfill the minimum standards of independence and impartiality.

214. The UN Human Rights Committee, when considering the UK periodic report under the ICCPR in July 2015, recommended the UK begin "ensuring that access to communication data is [...] dependent upon prior judicial authorization".[1207]

215. Recommendation:

1. Judicial Commissioners should authorize the obtaining of communications data.

Data Retention

Do the proposed authorisation regime and safeguards for bulk data retention meet the requirements set out in the CJEU Digital Rights Ireland and the Court of Appeal Davis judgments?

216. Part 4 regulates the retention of communications data. Under Clause 71 the Secretary of State can require any description of telecommunication operators to retain all or any description of communications data (and entity data) for up to 12 months. He or she may also impose requirements in relation to generating or processing the retained data (Clause 71.8). Retention of communications data is authorised by the Secretary of State only, with no judicial authorisation.

217. The blanket, untargeted retention of communications data provided for in the IP Bill is in breach of existing EU provisions protecting the right to privacy, such as the Data Protection Directive 1995/46 and the Directive on privacy and electronic communications 2002/58/EC. It is also a violation of applicable international human rights law, such as the EU Charter on Fundamental Freedom, the European Convention on Human Rights and the International Covenant on Civil and Political Rights.

218. The mandatory data retention regime under the IP Bill will go much further than

1205 See report of the UN Special rapporteur on the promotion and protection of the freedom of opinion and expression, UN doc. A/HRC/23/40, 17 April 2014; report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN doc. A/69/397, 23 September 2014, and report of the UN High Commissioner for Human Rights, Right to Privacy in the Digital Age, UN doc. A/HRC/27/37, 30 June 2014.

1206 See Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Judgment of 8 April 2014.

1207 Human Rights Committee, concluding observations on the UK, July 2015.

what was prescribed under the invalidated EU Data Retention Directive (2006/24/EC): for one, it will not only be limited to the detection or prevention of serious crimes, but for any of the ten grounds under which communication data can be requested (Clause 46.7).

219. The proposed retention regime also goes further than the types of data that can be retained under the current Data Retention Regulations 2014;[1208] there is a new retention requirement relating to the "pattern" of communications, and one related to "the internet protocol address, or other identifier, of any apparatus to which a communication is transmitted for the purpose of obtaining access to, or running, a computer file or computer program".[1209] Communications service providers may be required to retain not only data they save in their normal course of business, but also anything they may be able to generate or obtain, including ICRs.[1210]

220. As such, the IP Bill's proposed data retention regime will lead to the generation, collection, and storage, for up to a year, of highly revealing information pertaining to virtually all communications data sent, received or otherwise created by everyone. The retained data will potentially include, but also go well beyond, the who, what, where, when, and how relating to every communication that a person has online.

221. In Digital Rights Ireland v Minister for Communications and others, the Grand Chamber of the CJEU concluded that the 2006 Data Retention Directive (Directive 2006/24/EC of the Parliament and the Council of 15 March 2006), which required communications service providers to retain customer data for up to two years for the purpose of preventing and detecting serious crime, breached the rights to privacy and data protection under Articles 7 and 8 respectively of the EU Charter of Fundamental Rights.[1211]

222. The CJEU noted that the Directive was flawed for not requiring any relationship between the data whose retention was provided for and a threat to public security (see §59). The Grand Chamber concluded that the Directive amounted to a "wide-ranging and particularly serious interference" with the rights to privacy and data protection "without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary" (§65.)

223. The same concerns apply to the proposed data retention regime under the IP Bill.

224. Privacy International notes that on 20 November 2015 the Court of Appeal's judgment in the case of David Davis and others (to which Privacy International is an intervener) referred to the CJEU the question as to whether the requirements included in the Digital Rights Ireland's judgment are mandatory requirements with which the national legislation of EU member states must comply.

225. Privacy International believes that the Digital Rights Ireland requirements are mandatory and that existing EU law rules out data retention regimes of the kind proposed in the IP Bill. Irrespective of the decision of the CJEU on this matter, there is

1208 See: http://www.legislation.gov.uk/uksi/2014/2042/schedule/made
1209 See Clause 71(9)
1210 Clause 71, Part 4, Draft Investigatory Powers Bill
1211 Digital Rights Ireland v Minister for Communications and others, 8 April 2014, C-293/12.

growing consensus that the blanket retention of communications data, without suspicion, violates the right to privacy, as well as putting the security of personal data at risk of attack by criminals and others. In this context, it is notable that a significant number of European countries have moved away from blanket data retention regimes because of its incompatibility with EU law and the right to privacy.[1212]

226. Recommendation:

1. Delete Part 4 of the IP Bill and amend other parts accordingly. Instead of pursuing the regime of blanket retention of personal data, consider introducing "data preservation orders", under which the retention of specific individuals' communications data is requested by the authorities and authorised by judges.

Is accessing Internet Connection Records essential for the purposes of IP resolution and identifying of persons of interest? Are there alternative mechanisms? Are the proposed safeguards on accessing Internet Connection Records data appropriate?

227. ICRs offer no additional capability beyond that which is already available to an authority in regards of connecting an Internet Protocol (IP) address with a subscriber. Intellectual property rights holders have been connecting IP addresses to subscriber IDs for some time in cases where they wish to enforce their rights. They have done this by subpoenaing the provider of an IP address, which can be determined by who the address was allocated to, and serving a court order on the provider compelling them to release information in relation to their subscriber. This works reasonably well for fixed line communications. However in relation to a mobile phone communications it may be more complicated as there is no need to register a universal subscriber identity module (SIM) – the equivalent of a hard-ware embedded IP address for mobile phones – to an individual. It is nonetheless probably possible for the provider to know which SIM was registered to which cell (or tower(s)), and quite possibly to determine the location of the user of that SIM through the use of triangulation.

228. The main change the IP Bill would implement is that this and other data would need to be retained by telecommunication operators for up to 12 months (under Part 4).

229. The IP Bill definition of ICR is not technically crafted (see Clause 47(6)), making it impossible to assess exactly what an ICR would contain and who exactly would be required to retain them. Some more details can be glimpsed in the accompanying document "Operational Case for the Retention of Internet Connection Records".[1213] In this document a number of scenarios and case studies are explored and the justifications for ICRs are put forward.

1212 Even before the CJEU issued its judgment in *Digital Rights Ireland*, the constitutional or administrative courts of Bulgaria, Cyprus, the Czech Republic, Germany and Romania declared part or all of the relevant national legislation implementing the Data Retention Directive to be unlawful. Following the *Digital Rights Ireland* judgment, the courts of Austria, Slovenia, Belgium, Bulgaria, the Netherlands, Poland, Romania, and Slovakia have struck down national laws that had implemented or replicated the Data Retention Directive (or, in the case of Romania and Bulgaria, subsequent amendments to the original implementing laws).

1213 Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473769/Internet_Connection_Records_Evidence_Base.pdf

230. Privacy International notes that this document provides a very conservative view of the capabilities of that the IP Bill could potentially authorise as the vague nature of the language in the Bill could be interpreted to give considerably more information than this document suggests.

231. Further, the amount of data likely to be generated by capturing every port and IP combination of every connection, by every user in the United Kingdom and retaining that data for 12 months is likely to be a heavy burden upon telecommunication operators.

232. Recommendation:

    1. Clause 47: Delete subsections 47(4), (5) and (6)

    2. If data retention is to remain in the IP Bill, do not allow a retention order that would require telecommunications services to generate and retain ICRs.

Are the requirements placed on service providers necessary and feasible?

233. Clauses 71 and 79 empower the Secretary of State to require communications service providers to retain communications data (and entity data) for up to 12 months. This requirement is mandatory for providers located in the UK, and requested of those outside the UK. Requiring communications service providers to retain all of our revealing and personal data for 12 months treats us all as suspects, undermining the trust we place in government to only exercise its power to intrude upon on personal lives in the most limited and necessary of circumstances.

234. Due to the revealing nature of such data, the database(s) where this retained data is stored are also likely to be targeted by cyber criminals and foreign intelligence agencies. Compelled retention unnecessarily endangers the security of our data, as communications service providers could be subject to increased attacks to access that data. This year alone has seen the successful infiltration and hacking of several large databases. Recent examples include, but are not limited to, TalkTalk, Vodafone, British Gas, as well as the detrimental Office of Personnel Management (OPM) breach in the United States.[1214]

235. Clause 74 of the IP Bill imposes some general obligations to protect the security of such retained data, but its broad provisions are far from a guarantee that future attacks such as these would be prevented. Communications service providers bear the brunt of public criticism in the face of data breaches, even where they are being compelled to retain the data, further undermining trust in the security of their

1214 (27 February, 2015) Customer Data Stolen in TalkTalk Hack Attack, BBC Technology [Online] Available from: http://www.bbc.co.uk/news/technology-31656613 [Accessed 26 November, 2015], (31 October, 2015) Vodafone customers' bank details 'accessed in hack', company says, The Guardian [Online] Available from: http://www.theguardian.com/business/2015/oct/31/vodafone-customers-bank-details-accessed-in-hack-company-says [Accessed 26 November, 2015], Hern, Alex (29 October, 2015) British Gas denies responsibility for 2,200 user accounts posted online, The Guardian [Online] Available from: http://www.theguardian.com/technology/2015/oct/29/british-gas-denies-responsibility-user-accounts-posted-online-pastebin [Accessed 26 November, 2015], Hirschfeld Davis, Julie (9 July, 2015) Hacking of Government Computers Exposed 21.5 Million People, The New York Times [Online] Available from: http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html [Accessed 26 November, 2015]

services.

236. The IP Bill requires communications service providers to weaken their system security while simultaneously increasing the data they retain. This provides for a perfect storm that will make individuals' personal data far more susceptible to cyberattacks. As David Emm, principal security researcher at Kaspersky Lab points out, "[o]ne of the big issues is the practical aspects for ISPs – how are they going to store it, how is it going to provide access when required, and how secure will both of those things be?".[1215]

237. The new regime expands the scope of who could be served with a retention notice. Clause 193(10) defines "telecommunications operator" as a person who either offers or provides a telecommunications service to persons in the UK, or controls or provides a telecommunication system reaching the UK. The IP bill includes not just public telecommunications providers but also private networks. This will mean a very wide range of companies, from a large multinational telecommunication provider to a small tech startup would be subject to a notice.

238. The security concerns raised by retention would be felt not only within the technology sector, but also within related businesses that rely on secure communications and customer trust. Many of these businesses contribute greatly to the British economy, and include the banking, financial, and legal sector, as well as the computer software, hardware, anti-virus, gaming, and start-up industries.

239. Individuals will consequently face a reduction in their privacy and security, which could undermine trust in the entire communications system. The internet offers a democratic space in which personal exploration, growth, change, and development is possible, and without trust in the systems that enable such exploration, such positive growth is curtailed.

240. Recommendation:

    1. Delete Part 4 of the IP Bill and amend other parts accordingly. Instead of pursuing the regime of blanket retention of personal data, consider introducing "data preservation orders", under which the retention of specific individuals' communications data is requested by the authorities and authorised by judges.

Equipment Interference

Should the security and intelligence services have access to powers to undertake (a) targeted and (b) bulk equipment interference?

241. For the first time in the UK, the draft IP Bill includes statutory provisions describing the power of law enforcement and the intelligence services to hack into our computers. This power is called "Equipment Interference", and is detailed in Part 5 and, as a "bulk" power, in Part 6, Chapter 3.

1215 Allison, P.R. What the Investigatory Powers Bill means for the telecommunications industry, *Computer Weekly* [Online]. Available from http://www.computerweekly.com/feature/What-the-Investigatory-Powers-Bill-means-for-the-telecommunications-industry [Accessed 15 December 2015]

242. Hacking, as undertaken by any actor, including the state, fundamentally impacts on the security of computers and the internet. It incentivises the state to maintain security vulnerabilities that allow any attacker – whether GCHQ, another country's intelligence agency or a cyber criminal – potential access to our devices. Hacking can undermine the security of all our communications, whether we are emailing our loved ones or banking online. One US intelligence official analogised using hacking to a situation in which "[y]ou pry open the window somewhere and leave it so when you come back the owner doesn't know it's unlocked, but you can get back in when you want to."[1216]

243. Privacy International has written extensively on the security concerns raised by hacking, and as have security experts. We do not repeat those submissions here, but include some of them for your reference.[1217] If hacking is to be used by the state, these security concerns must be addressed.

244. As currently drafted the IP Bill compounds these security concerns by forcing telecommunications services to become complicit in government hacking. Clause 99 requires any person (which could include CSPs) to "provide assistance in giving effect to the [equipment interference] warrant." Clause 101 explicitly applies this duty to "relevant telecommunications providers." Under these two clauses, communications service providers could be compelled to take any steps, unless "not reasonably practicable", to assist the police and the intelligence services to hack our computers and other devices.

245. While we do not know what this assistance will look like in practice, it might include compelling telecommunications services to send false security updates to a user in order to install malware that the police or intelligence services could then use to control the user's computer. As we explained to the Science & Technology Committee, the possibility that security updates might be co-opted would undermine trust in those updates, which are crucial to protecting our devices from unauthorised intrusions from criminals.[1218] The general public is likely never to be made aware of what kind of "hacking" assistance has been required of telecommunications providers due to the very strict non-disclosure provision in the IP Bill (Clause 102). It will therefore be very hard to maintain trust if Clauses 99 to 102 remain in the IP Bill.

1216 Gellman, B. and Nakashima, E., U.S. spy agencies mounted 231 offensive cyber- operations in 2011, documents show, *The Washington Post* (30 August 2013), available at: https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html

1217 Please see: Privacy International and Open Rights Group's Submission in Response to the Consultation on the Draft Equipment Interference Code of Practice (20 March 2015), available at: https://www.privacyinternational.org/sites/default/files/PI%20and%20ORG%20Submission%20-%20Draft%20Equipment%20Interference%20Code%2020%20Mar%202015_0.pdf ; Privacy International Submission in Response to Science & Technology Call for Evidence on the Draft Investigatory Powers Bill (27 November 2015) [hereinafter "PI & ORG Science & Technology Committee Submission"], available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25170.html ; Expert Report of Professor Ross Anderson, submitted in Privacy International and Greennet Limited et al. in the Investigatory Powers Tribunal (Case nos. IPT 14/85/CH and 14/120-126/CH) (30 September 2015), available at http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25170.html

1218 PI & ORG Science & Technology Committee Submission, paras. 22-23.

246. Hacking is also an incredibly intrusive form of surveillance. When an agent takes control of a computer by hacking it, there are few limits on what can be done.[1219] Unlike intercept capabilities, hacking capabilities can be deployed in any number of configurations to do any number of different things. The logging of keystrokes, tracking of locations, covert photography, and video recording of the user and those around them enables intelligence agencies and the police to conduct real-time surveillance. Anything we store on our computers and mobile phones, intentionally or unintentionally, is also fair game, from location records, to saved documents and notes, to draft messages and emails, and more. As "smart" technology develops, hacking will increasingly provide access to our refrigerators and thermostats, our children's dolls and our cars.

247. Because of its intrusiveness, hacking should only be deployed under the strictest authorisation regime, with stringent safeguards and vigorous oversight. Unfortunately, the draft IP Bill fails to provide these. In particular, as discussed above in paragraphs 67 to 79, the "targeted" equipment interference powers in Part 5 are not in fact targeted but can be deployed in bulk using thematic warrants.

248. Bulk equipment interference, whether carried out under a thematic warrant or under the explicit "bulk" power in Part 6, Chapter 3, destroys the ability of the authorising authority to assess the necessity and proportionality of the hacking being undertaken. Without knowing which computer is to be hacked into – as well as what information might be contained on that computer, who else might be using it, the level of suspicion that attaches to the person or people who might be using the computer, etc. – how can a Judicial Commissioner properly assess if such intrusion is proportionate? Indeed, the Grand Chamber of the European Court of Human Rights recently declared that an authorisation for surveillance must identify "a specific person" or "a single set of premises" in order to facilitate the necessity and proportionality analysis.[1220]

249. "Bulk" hacking under Part 6, Chapter 3 is permitted only where the main purpose of the warrant is to obtain "overseas-related" communications, private information and equipment data. This limitation should provide little comfort for those residing in the UK. For instance, much of our data is stored overseas in servers operated by telecommunications services such as Google and Facebook. Given how intrusive hacking is, and how our interconnected world makes it just as easy to hack a computer in Belgium as in Birmingham, drawing a distinction between overseas hacking and internal hacking makes little sense. Equipment interference should only be authorised where a specific target has been identified, and a very strong case has been made as to the necessity of obtaining the information sought from the target.

250. Finally, because hacking involves an active interference with a computer, it raises serious evidentiary concerns. Evidence obtained via equipment interference is admissible in court. Once an agent or officer takes control of a computer by hacking

---

1219 For an overview of the types of information that can be obtained via hacking, please see the Expert Report of Peter Michael Sommer, submitted in Privacy International and Greennet Limited et al. in the Investigatory Powers Tribunal (Case nos. IPT 14/85/CH and 14/120-126/CH) (30 September 2015) [hereinafter Sommer Report], available at: https://www.privacyinternational.org/sites/default/files/PI_PMS_Report_final.pdf

1220 Zakharov v Russia 47143/06, 4 December 2015, at paras. 259-267.

it, however, they have the unfettered ability to alter or delete any information on that device. This raises the risk, in the context of a criminal prosecution, of defence accusations of evidence tampering.[1221] The IP Bill currently does not contain any provisions to address this evidentiary concern. Without such safeguards, the efficacy of the use of hacking in investigating and prosecuting crimes is very questionable.

251. Recommendations:

1. Thoroughly assess the security concerns raised by equipment interference to determine if they can be resolved.

2. Delete clauses 99 to 102.

3. Implement changes recommended above (paragraph 78) to clause 83.

4. Delete Part 6, Chapter 3.

5. Include provisions to address the evidentiary concerns raised by equipment interference.

252. Questions:

1. What sort of "assistance" in interfering with equipment might be required under clauses 99 and 101?

2. How can proportionality be assessed when a thematic warrant or a bulk warrant is being authorised?

Should law enforcement also have access to such powers?

253. Granting law enforcement access to equipment interference powers has the potential to compound security concerns as it will likely increase both the number of devices that will be hacked and the number of officers who will be doing the hacking. For the same reasons stated above, therefore, careful consideration should be given to whether hacking is an appropriate police power in light of the security threat.

254. Hacking for law enforcement purposes also brings the evidentiary problems, discussed in response to the previous question, to the fore. Allowing law enforcement to hack makes the need to address these evidentiary concerns even more pressing.

Are the authorisation processes for such equipment interference activities appropriate?

255. As we contend throughout this submission, intrusive powers such as equipment interference must be subject to robust, independent judicial authorisation (see, e.g., our response to the question "Is the authorisation process appropriate?").

256. Additionally, Privacy International has established ten principles we believe must be met if equipment interference is to be a permitted power. Those principles are

1221 For a more extensive discussion of these evidentiary concerns, please see Sommer Report at paras. 108-111.

outlined in our submission on the draft Equipment Interference Code of Practice.[1222]

257. The Sixth Principle sets forth many of the elements we believe should be included in a warrant to ensure effective and human rights compliant authorisation of equipment interference. These include:

1. the specification of an individual target;
2. a statement of the nature of the suspicion that the target is connected to a serious crime or a specific threat to national security;
3. a declaration with supporting evidence that there is a high probability evidence of the serious crime or specific threat to national security will be obtained by the operation authorised;
4. a precise and explicit description of the method and extent of the proposed intrusion and the measures taken to minimise access to irrelevant and immaterial information;
5. a declaration with supporting evidence that all less intrusive methods of obtaining the information sought have been exhausted or would be futile;
6. a declaration with supporting evidence that the security of the device targeted or communications systems more generally will not be negatively impacted by the proposed intrusion; and
7. a time limit of one month, although the warrant may be renewed on a monthly basis with sufficient cause, including an explanation of why the information sought has not yet been obtained.

258. None of these elements are included in equipment interference warrants currently proposed in the IP Bill. Indeed, thematic warrants and bulk warrants completely lack any elements of individualized suspicion, and necessarily would not be able to specify the extent of the proposed intrusion given the target is unknown. Nor is there a requirement that hacking be a method of last resort; the Secretary of State need only "take into account" whether the information sought "could reasonably be achieved by other means" (Clause 84(6)). Finally, equipment interference warrants last for 6 months (Clauses 94 and 141).

259. Given how technically complex equipment interference can be, the Judicial Commissioners should have technically competent assistance so they can fully understand and consider the nature of the intrusion being proposed.

260. <u>Recommendations</u>

1. If there is to be the power of equipment interference, require equipment interference warrants to contain the elements listed above, potentially by amending clause 93.

1222 PI and ORG Consultation Response: Draft EI Code, at pages 9-15.

2. Ensure Judicial Commissioners have technically competent assistance in order to fully vet warrants.

Are the safeguards for such activities sufficient?

261. Authorisation is one of the most important safeguards for equipment interference. As we argue above, the authorisation regime needs significant improvement. We add to that concern two problems we see with the safeguards proposed in clauses 103 (equipment interference) and 146-147 (bulk equipment interference).

262. First, if information obtained through equipment interference is to be shared outside the agencies or organization that originally obtained the information, including with overseas authorities, that sharing should be very closely circumscribed in law. The draft IP Bill fails to provide such protections.

263. Instead, clause 103 does not even mention possible overseas sharing. Yet clauses 103(3)-(4) and (8) appear broad enough to allow it. In contrast, clause 146(8) references sharing material acquired via bulk equipment interception with "authorities of a country or territory outside the United Kingdom."

264. Clause 146(8) also illustrates the problems with such sharing by removing the safeguards contained in clauses 146(3) (minimizing copying and disclosure of data) and 146(6) (destruction of data) when the data is handed over to overseas authorities. Presumably, these protections are removed because once the data is shared the UK authorities will no longer have effective control over it. This lack of future controls means that if information is to be shared, it must only be in the most limited of circumstances where there is a strong and demonstrable justification for the sharing, and the UK has confidence that the overseas authority that will be receiving the information will not use it for improper purposes (clause 146(9) is not sufficient in this regard). The UK should also negotiate the right to continuing oversight of how the information is used.

265. Also of note, the IP Bill fails to regulate how the UK authorities should treat information obtained by other countries via equipment interference that is then shared with the UK. This is a significant oversight, as such a lack of publicly accessible policies on sharing was found to be unlawful in the context of interception.[1223] As discussed above in paragraphs 53 to 54, how the IP Bill addresses overseas sharing needs significant improvement.

266. Second, notification is a common safeguard in warrantry systems around the world.[1224] The presumption is that the target of surveillance will be notified when

[1223] See Liberty & Others v the Secretary of State (2015) UKIPTrib 13_77-H, at para. 23, available at: http://www.ipt-uk.com/docs/Liberty_Ors_Judgment_6Feb15.pdf

[1224] Consider the following examples:

- Canada: Section 196.1 of the Canadian Criminal Code requires notification to the target of the interception "within 90 days after the day on which it occurred" subject to extension.
- Germany: Section 101 of the German Code of Criminal Procedure articulates a duty to inform targets of surveillance and others who might have been affected "as soon as it can be effected without endangering the purpose of the investigation, the life, physical integrity and personal liberty of another, or significant assets".
- Japan: The Act on the Interception of Communications provides that the target of intercepted communications must be notified within 30 days of the completion of surveillance subject to extension. *See* UNODC, *Current Practices in*

there is no risk of jeopardising an ongoing investigation. This should ordinarily happen within 12 months of the conclusion of the investigation, although that 12-month period may be extended in six-month intervals by judicial authorisation. The draft IP Bill lacks any such presumption of notification.

267. Recommendations

1. Explicitly address sharing of information obtained via equipment interference with overseas authorities (and from overseas authorities to the UK) and strengthen the safeguards that attach to sharing.

2. Include provisions requiring notification of subjects of surveillance when there is no risk of jeopardising an ongoing investigation.

268. Questions

1. Why is sharing with overseas authorities explicitly addressed in the context of bulk equipment interference (Part 6, Chapter 3) but not for regular equipment interference (Part 5)?

2. Why doesn't the IP Bill address the sharing with UK agencies of data obtained via equipment interference by overseas authorities?

3. Why doesn't the IP Bill include notification provisions?

Bulk Personal Data

Is the use of bulk personal datasets by the security and intelligence services appropriate?

269. This answer to the particular aspects of the Bulk Personal Dataset regime should be read in conjunction with Privacy International concerns and objections to the bulk warrants mentioned above.

270. The acquisition, retention and use of Bulk Personal Datasets involves obtaining a set of information that includes personal data relating to a number of individuals, who, as the IP Bill notes, are of not of interest to the intelligence service in the exercise of its functions (Clause 150.) These datasets can be obtained from other public sector bodies or from the private sector.

271. Bulk Personal Datasets can be obtained in two ways, through a specific BPD warrant (Clause 154) and a class BPD warrant (Clause 153). A class BPD warrant authorises an intelligence service to obtain, retain or examine bulk personal datasets that fall within a class described in the warrant. A class warrant must include a description of the Bulk Personal Datasets to which it relates and an explanation of the operational

Electronic Surveillance (2009), at page 17, available at https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf.

- US: At the federal level, § 2518(8)(d) of the Wiretap Act (18 U.S.C. §§ 2510-2522) requires notification to targets of surveillance and "such other parties . . . as the judge may determine in his discretion that is in the interest of justice" within "a reasonable time but not later than ninety days after . . . the termination of . . . the [surveillance] order". Notification that an application for such an order was sought but denied is also required to the same parties within the same time frame.

purpose for which the applicant wishes to examine the data collected. No further guidance is provided as to the kind of terms that would suffice to sufficiently describe a class of Bulk Personal Datasets. The case law of the European Court of Human Rights is clear that the minimum safeguards that should be set out in law in order to avoid abuses of power include a definition of the categories of people liable to have their data recorded and retained.[1225] Clause 153 fails to provide detailed rules governing the scope of class BPD warrants.

272. Furthermore, as we discuss in paragraphs 88-90, once the datasets have been obtained there are not sufficient limitations on how they may be examined.

273. Clause 154 relating to a specific BPD warrant is not any better, as while a specific dataset must be specified in the warrant, there are no limitations on what that dataset might contain or where it might be obtained. Like the other bulk powers, we believe these problems mean that Part 7 should be removed from the Bill. We are bolstered in our suggestion by the fact that the Home Office has yet to make a strong operational case for the BPD power.

274. Recommendations:

1. Delete Part 7

Are the safeguards sufficient for the retention and access of potentially highly sensitive data?

275. If the power to obtain Bulk Personal Datasets remains in the IP Bill, we reiterate the concerns we expressed above in paragraphs 186-188 with regard to security problems created by the retention of large amounts of sensitive personal information.

276. In addition, as pointed out in paragraph 90 above, there are few safeguards on who can access BPDs after they have been collected. This is a failing of the section and inconsistent with the protections placed on the other bulk powers.

Oversight

What are the advantages and disadvantages of the proposed creation of a single Judicial Commission to oversee the use of investigatory powers?

277. Privacy International commends the IP Bill's attempt to simplify what was formerly a "confusing array of mechanisms, with little clarity as to the demarcation between them".[1226] Both the Anderson and RUSI Reports documented the concerns raised from many quarters regarding the opacity and unnecessary complexity of a proliferating number of oversight mechanisms and regulators.[1227] As a result, both

1225 See S and Marper v United Kingdom (2009) 48 EHRR 50, at §99: "[The Court] reiterates that it is as essential…secret surveillance and covert intelligence-gathering to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness."

1226 Anderson Report, para. 12.79.

1227 *Id*.; RUSI Report, paras. 4.42-43.

reports also recommended the creation of a single oversight mechanism that would merge the functions of the Intelligence Services Commissioner, Interception of Communications Commissioner's Office and Office of Surveillance Commissioners.[1228] A main advantage of the draft IP Bill is the acceptance of this recommendation through the creation of the Investigatory Powers Commissioner.

278. We are concerned, however, that a single Commission will be responsible for conducting both authorisation and oversight and consider this to be a critical flaw in its current form. Authorisation is a distinctly legal function. While we take issue with the judicial review standard to be applied by the Judicial Commissioners in the draft IP Bill, we emphasise here that their role is to make a judicial determination on the legality of a warrant application. By contrast, oversight demands a fundamentally different set of skills, which the Judicial Commissioners should not be tasked to undertake.

279. This distinction is documented nicely in the RUSI Report, which noted the following criticism of the current Commissioners:

> "[T]hey are judges, not investigators. They are . . . generally less experienced in identifying problems of process or the application of new technology. . . . [T]he commissioners need to be 'inquisitive troublemakers', with a level of investigatory expertise that is prized by the agencies themselves. There is a need for individuals . . . who can . . . question and challenge people and practices within the relevant organisations. Given the depth of investigations . . . the commissioners require greater assistance from teams of people with appropriate skills and expertise, perhaps in the form of legal and technical 'juniors'."[1229]

280. Fusing the authorisation and oversight functions into a single Commission also raises serious conflict of interest concerns. The draft IP Bill essentially proposes that the Commission both participate in authorising warrants and undertake reviews of that very authorisation process. We believe that this structure cannot provide the independence that is so critical to a functioning oversight system.

281. We bring to the Committee's attention that neither the ISC nor RUSI recommended the merging of the authorisation and oversight functions in the manner proposed by the draft IP Bill. In particular, RUSI emphasised that "[t]he judicial commissioners in charge of the authorisation of warrants should not be part of a new [oversight mechanism]".[1230] It further explained that the oversight mechanism should cover "four main areas of responsibility: inspection and audit, intelligence oversight, legal advice, public engagement".[1231] We note that one of Anderson's own models for the new oversight mechanism proposes that a "Chief Judicial Commissioner" be responsible for authorisation while a separate "Chief Commissioner (non-judge)" be responsible for oversight.[1232]

1228 Anders Report, Recommendation 82; RUSI Report, Recommendations 17-19.
1229 RUSI Report, paras. 4.80-83.
1230 RUSI Report, para. 5.60.
1231 RUSI Report, Recommendation 18.
1232 Anderson Report, Annex 18.

282. Recommendation:

1. Separate the authorisation and oversight functions that are currently combined in a single Judicial Commission.

Would the proposed Judicial Commission have sufficient powers, resources and independence to perform its role satisfactorily?

283. Powers - Privacy International submits that the Investigatory Powers Commission does not have adequate judicial authorisation powers in the draft IP Bill. The draft Bill preserves the power of the Secretary of State to issue warrants while permitting Judicial Commissioners to "review" this decision (see in particular Clauses 19-21, 59, 90, 109, 123, 138, 155). Above we provide criticism of this proposed authorisation system in response to the question "Is the authorization process appropriate?"

284. Privacy International is also concerned that judicial authorisation, even in the weak form expressed in the draft IP Bill, is not required for a range of powers that interfere with the right to privacy. In our prior submission to the Joint Human Rights Committee, we outlined these powers, which include obtaining communications data, issuing data retention notices and modifying interception warrants.[1233] We also articulated that the lack of judicial authorisation for such powers may fall short of requirements under international human rights law.

285. Resources - The Anderson, ISC and RUSI reports all emphasised the need to ensure that the surveillance oversight mechanisms – whatever form they should take – are well-resourced.[1234] We reiterate that position with respect to both authorisation and oversight, which as we explain above must remain separate from each other. In terms of authorisation, we highlight the need to ensure that there is an adequate number of Judicial Commissioners. While we do not think that the Secretary of State must play a role in authorising warrants, we note the criticism levied at the sheer number of warrants she and her predecessors have been asked to authorise under the current system.[1235] With respect to oversight, we urge the Committee to consider the resources necessary "to compare practice across the whole range of different public authorities", "to inspect the whole range of surveillance techniques", "to attract excellent specialists", and to enhance the public profile of such work.[1236] For both authorisation and oversight, we highlight the critical importance of technical expertise.

286. Clause 176(2) articulates that the Secretary of State is to provide the Judicial Commissioners with the staff and "accommodation, equipment and other facilities" she "considers necessary for the carrying out of the Commissioners' functions". We question the appropriateness of granting the Secretary of State the power to determine the resources of the Investigatory Powers Commission as it may

1233 *Id*. at paras. 51-56.
1234 *See* Anderson Report, paras. 14.94-97; ISC Report, para. 211; RUSI Report, para. 5.66.
1235 *See* Big Brother Watch, Joint Committee on the Draft Investigatory Powers Bill – Written Evidence, Dec. 2015, pages 3-4, available at https://www.bigbrotherwatch.org.uk/wp-content/uploads/2015/12/Draft-Investigatory-Powers-Bill-Consultation-Big-Brother-Watch-Response.pdf; Anderson Report, para. 7.33 (noting that the Home Secretary personally authorised "2,345 interception and property warrants and renewals" in 2014).
1236 Anderson Report, para. 14.97.

undermine its independence. We would also urge the Committee to consider adding more precise language to this clause laying out the types of resources, in particular technical expertise, to be provided to the Commission.

287. Independence - Privacy International submits that the proposed IP Commission is not sufficiently independent to perform its role satisfactorily. First, the appointment of Judicial Commissioners by the Prime Minister, rather than through the Judicial Appointment Commission, subverts the very independence that their participation is meant to bring to the authorisation process (Clause 167(1)). Permitting the executive to appoint the Commissioners inappropriately blurs the line between the branches, risking political bias on the part of the Commissioners.[1237] This concern is exacerbated by the three-year terms of office for Commissioners proposed by the draft IP Bill (Clause 168(2)). The brevity and renewable nature of these terms renders the Commissioner role inherently insecure, increasing the risk that their decisions will be biased towards the executive.

288. Second, the draft IP Bill further undermines the independence of Judicial Commissioners by permitting the Secretary of State to appeal refusals to approve a warrant or authorisation to the IP Commissioner (Clauses 19(5), 109(4), 123(4), 138(4), 155(3)). The right to appeal is not constrained in any way and simply gives the Secretary of State a second bite at the apple if displeased with the decision of a Judicial Commissioner. This right is particularly troubling given the executive influence in appointing the Judicial Commissioners, including the IP Commissioner, discussed above.

289. Recommendations:

1. Vest the power to issue warrants in Judicial Commissioners or, in the alternative, remove the "judicial review" standard in the approval clauses.

2. Ensure prior judicial authorisation for the acquisition of communications data and the modification of interception warrants.

3. Consider granting the power to determine resources for the Judicial Commission to an authority other than the Secretary of State.

4. Consider adding more specific language to Clause 176(2) to require particular resources, especially technical expertise, be provided to the IP Commission.

5. Ensure Judicial Commissioners are independently appointed by the Judicial Appointments Commission and serve fixed-length terms.

Are the appointment and accountability arrangements for Judicial Commissioners appropriate?

290. As we state in the preceding section, we think the Judicial Appointment Commission should appoint Judicial Commissioners, not the Prime Minister. Further, the

1237 While Anderson observed that "[t]he Chief Commissioner should be appointed by the Prime Minister", he at least suggested that "[c]onsideration . . . be given to allowing the ISC a voice in the appointment or confirmation of the Chief Commissioner." He did not indicate how Judicial Commissioners, sitting under the Chief Commissioner, should be appointed. Anderson, Recommendation 105.

Secretary of State's ability to appeal a decision of a Judicial Commissioner should be circumscribed so as not to merely give him or her a "second bite at the apple."

Are the new arrangements for the Investigatory Powers Tribunal including the possibility of appeal adequate or are further changes necessary?

291. The Investigatory Powers Tribunal is an important yet imperfect component of the oversight regime. The IPT and its procedure are handicapped in several ways that, if remedied, could improve the openness and fairness of the process through which claims against the intelligence services are adjudicated.

292. The IPT should operate under a presumption of openness unless a compelling case is made that allowing specific information to be made public would harm national security. To facilitate this openness, we recommend the IP Bill be amended to:

    1. Include a presumption of openness;

    2. Require any party requesting a closed hearing or to submit closed evidence to provide the national security reasons for the request to the IPT (opposing parties should also be made aware of the existence of the request); and

    3. Require the IPT to determine if a request for a closed hearing or to submit closed evidence is justified on national security grounds, while also giving the IPT the related power to compel the production of evidence if there are not sufficient reasons to keep it secret. There should be an especially strong presumption in favour of the production of internal policies and legal interpretations given how important they are to a full consideration of the lawfulness of the intelligence services' activities.

293. Where portions of a proceeding cannot be held in open because of the harm to national security, the IPT must appointment a Special Advocate to represent the interests of any excluded party in the closed sessions.

294. While the ability to appeal an IPT decision is a welcome change, the right to appeal proposed in the Bill is a limited one. For instance, an appeal may only be taken with leave of the IPT or the court that will hear the appeal (Clause 180(3)). Not every issue can be appealed – only those which are deemed to "raise an important point of principle or practice" or where there is "another compelling reason for granting leave" (Clause 180(4)). Careful consideration should be given to whether such limitations are appropriate. In the context of other tribunals, appeals are permitted where they would have a real prospect of success; or there is some other compelling reason why the appeal should be heard.[1238]

295. <u>Recommendations</u>

    1. The IPT should operate under a presumption of openness.

    2. Any request for a closed hearing or to submit closed evidence must be justified to the IPT on national security grounds. The IPT must them determine if the request

[1238] See CPR 52.3(6), available at: https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part52

if justified.

3. The opposing parties should be made aware of the existence of any request for a closed hearing or to submit closed evidence.

4. The IPT should have the power to compel the production of evidence if there are not sufficient reasons to keep it secret.

5. The IPT must appoint a Special Advocate who can represent the interests of any excluded party during closed sessions.

6. Appeals from the IPT should be allowed where they would have a real prospect of success; or there is some other compelling reason why the appeal should be heard.

21 December 2015

Public Concern at Work—written evidence (IPB0077)

We welcome the opportunity to contribute to the consultation process for the Draft Investigatory Powers Bill (DIPB).

Background

1. By way of introduction, Public Concern at Work (PCaW) is an independent charity and legal advice centre. The cornerstone of the charity's work is a confidential advice line for workers who have witnessed wrongdoing, risk or malpractice in the workplace but are unsure whether or how to raise their concern. The advice line has advised over 18,000 whistleblowers to date; this unique insight into the experience of whistleblowers informs our approach to policy and campaigns for legal reform.

2. The charity has been closely involved in the operation of the law that protects whistleblowers, the Public Interest Disclosure Act 1998 (PIDA) since its inception and campaigned to put it on the statute books in the 1990's.

3. PIDA, while essential legislative protection, is only one part of the framework in the UK that is needed to ensure whistleblowing is safe and effective. To this end in February 2013 PCaW established the Whistleblowing Commission to examine the effectiveness of whistleblowing in the UK and to make recommendations for change.

4. The Whistleblowing Commission published its report in November 2013.[1239] The key recommendation of the Commission is the creation of a statutory Code of Practice which sets out the key principles for effective whistleblowing which can be taken into account by courts and tribunals considering whistleblowing claims. The Commission also recommended that this Code could be used by regulators as part of their inspection and assessment regimes.

5. This short response will focus on reforming the whistleblowing framework for the UK intelligence service as part of an effective system of accountability for the new powers that the DIPB will create.[1240] Our proposed reforms are based on the Tshwane Principles, a set of global principles that balances the need to maintain the secrecy of information relating to national security, while ensuring that wrongdoing or malpractice is reported and dealt with where it arises.[1241] Annex 1 includes a draft amendment for DIPB that follows the Tshwane Principles.

Definitions

6. The following contribution refers to "whistleblowing", "whistleblowers" or "raising concerns". All three concepts refer to individuals reporting wrongdoing, risk or malpractice either internally (i.e. to their line manager, senior manager or Board) or

[1239] The Whistleblowing Commission report, November 2013- http://www.pcaw.org.uk/files/WBC%20Report%20Final.pdf
[1240] See Annex 1 for a suggested amendment to the current bill.
[1241] For more information about the Tshwane Principles see: https://www.opensocietyfoundations.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles

externally (i.e. to regulators, MPs and the media) where the individual has witnessed wrongdoing or malpractice in their place of work. The critical point being that this activity is encouraged, and usually starts, at line management level.

7. The legal protection for whistleblowers in the UK is to be found in the Public Interest Disclosure Act 1998 (PIDA), which provides compensation through the employment tribunal where a worker has been dismissed, forced out of their job or suffers some other form of victimisation from either their employer or co-workers because they have made a qualifying protected disclosure.

8. In summary, a disclosure will 'qualify' for protection where, in the reasonable belief of the worker, the information is in the public interest and tends to show one or more of a number of listed 'wrongdoings'. There are additional requirements where the disclosure is made to a body or person other than to the employer.

9. In the context of the issue at hand, it is of significance that the qualifying disclosure will not be protected if by making the disclosure the worker commits an offence such as breaching the Official Secrets Act or commits the offence of Misconduct in Public Office.

10. *Disclosure to an employer:* Disclosure of information by a worker will be protected if the worker makes a qualifying disclosure to the employer or, in certain circumstances, to a Minister of the Crown.[1242]

11. *Disclosure to a regulator:* Disclosure of information by a worker will also be protected if the worker makes a qualifying disclosure to a 'prescribed person', reasonably believing that the information and any allegation contained within it are substantially true. The Secretary of State (in practice the Secretary of State for Business, Innovation and Skills) prescribes by list both the identity of the prescribed person (usually a regulatory body) and its remit. The list can be found in a series of statutory instruments. The worker wishing to make a protected disclosure risks losing protection if the report is to a regulatory body not on the list and/or the worker makes a report in respect of a matter outside the prescribed remit. [1243]

12. *Disclosure to the wider public:* Disclosure of information by a worker will also be protected if the worker makes a qualifying disclosure to any person or body provided that a number of detailed further conditions are satisfied. These conditions include a requirement that the worker does not make the disclosure for purposes of personal gain and a requirement that it is reasonable to make the disclosure in the circumstances. A further section makes provision for a qualifying disclosure of an exceptionally serious failure to any person or body. Again, a number of detailed conditions apply.[1244]

[1242] S.c. 43C the Employment Rights Act 1996
[1243] S.c. 43F the Employment Rights Act 1996
[1244] S.c. 43G the Employment Rights Act 1996

Whistleblowing protection for members of the UK intelligence community and members of the armed forces

13. We have limited this response to the issues that surround the disclosure of information by Public Personnel who deal with sensitive and/or classified information as it is highly likely that these individuals will not currently be covered by the statutory framework provided by PIDA. While the law already protects workers within law enforcement bodies (police officers and civilian staff) who will also be using the new interception powers, this contrasts sharply with the legal situation for intelligence personnel where any disclosure arrangements are neither available for public scrutiny nor underpinned by law. The DIPB provides this committee with an opportunity to address this anomaly, improve the accountability of any new interception powers, whilst balancing the legitimate need to withhold information on national security grounds.

14. Members of the intelligence community (along with members of the armed services) are excluded from the protection afforded by PIDA[1245] and as stated above, PIDA provides no legal protection to any worker outside the intelligence community who commits a criminal offence when raising their concern.[1246] This means that any disclosure of information that falls within the Official Secrets Act 1989 (OSA) is not protected.

15. It is also very difficult to judge whether there are effective arrangements in place for intelligence personnel to raise concerns internally (to managers within their place of work) and whether these are periodically reviewed, as these arrangements are neither publically available nor accessible via Freedom of Information Laws.[1247]

16. There is considerable uncertainty regarding whether intelligence personnel are protected from criminal prosecution under the OSA for raising concerns with existing external channels such as the Intelligence and Security Committee of Parliament (ISC).

17. The judge in the prosecution of former MI5 officer David Shayler suggested that members of the intelligence service could approach the ISC or the Intelligence and Surveillance Commissioners with concerns.[1248] The ISC has powers to protect witnesses that appear before the committee:

> *"(1) Protection for witnesses 7(1) Evidence given by a person who is a witness before the ISC may not be used in any civil or disciplinary proceedings, unless the evidence was given in bad faith.*
>
> *(2) Evidence given by a person who is a witness before the ISC may not be used against the person in*

[1245] S.c. 193 the Employment Rights Act 1996
[1246] S.c. 43B the Public Interest Disclosure Act 1998
[1247] https://www.leighday.co.uk/News/2014/September-2014/Five-Eyes-Surveillance-treaty-challenged-at-the-EC
[1248] 3, p.g. 1, Rv Shayler [2001] EWCA Crim 1977

any criminal proceedings, unless the evidence was given in bad faith." [1249]

18. These provisions protect an individual where they appear before the ISC and protect the evidence they give but do not appear to provide protection before this point, for the initial contact or where the individual raises a concern with the ISC but doesn't appear before them as a witness.

Public Interest Disclosures by the members of the UK intelligence community

19. Better clarity and assurances can be given to intelligence personnel by creating a clearer internal framework for intelligence personnel to use when raising concerns and good legal protection when public interest information is disclosed outside of the internal framework. This should also recognise the need to withhold information on the grounds of national security.

Categories of Wrongdoing

20. Given the important and sensitive work the intelligence community carries out we would suggest that any whistleblowing provisions within the DIPB should carefully identify what wrongdoing can be reported through the internal whistleblowing arrangements.

21. Principle 37 of the Tshwane Principles provides a carefully considered list of categories of wrongdoing that can be disclosed through the whistleblowing arrangements regardless of the security classification or the level of confidentiality attributed to the information. This list includes the following categories of wrongdoing or malpractice:

> (a) criminal offenses;
> (b) human rights violations;
> (c) international humanitarian law violations;
> (d) corruption;
> (e) dangers to public health and safety;
> (f) dangers to the environment;
> (g) abuse of public office;
> (h) miscarriages of justice;
> (i) mismanagement or waste of resources;
> (j) retaliation for disclosure of any of the above listed categories of wrongdoing; and
> (k) deliberate concealment of any matter falling into one of the above categories.'[1250]

The Disclosure Regime

[1249] Schedule 1 (7) Protection for Witnesses, the Justice & Security Act 2013.
[1250] Principle 37 of the Tshwane Principles, p.g.49.

22. We would suggest that the DIPB require intelligence agencies to put in place internal procedures and designate persons within them to receive concerns. This recommendation is in line with Principle 39 of the Tshwane principles.[1251]

23. *Internal Disclosures:* For a whistleblowing framework to be effective there needs to be an internal process that encourages staff to raise concerns with line managers as a sensible first step but should also recognise that this can be bypassed where necessary. Good arrangements will include a variety of options internally beyond line management so that where raising the concern with a line manager is not an option or a sensible course of action (e.g. where the line manager is implicated in the wrongdoing), or where the concerns have been raised locally but the concerns remain unaddressed, it should be clear that the concern can safely be raised at a higher level.[1252]

24. *Independent Oversight:* The role of external oversight is important to reassure staff, other stakeholders and the public that the intelligence community intends to deal with any malpractice properly. We would suggest that given there will likely be a judicial committee overseeing the use of powers under the DIPB, this committee could also take the role of an independent oversight body within the whistleblowing arrangements for the intelligence services. We also recommend that any legal framework takes into account the role of the JSC and includes them as an external point of contact as well.[1253]

25. There should be duty on the oversight body receiving the concern to:

> 1) investigate the wrongdoing and take prompt action;
> 2) protect the identity of the individual where the concerns have been raised in a confidential manner and anonymous concerns (where the identity of the employer is unknown) are considered on their merits;
> 3) protect the information disclosed and the fact a disclosure has been made except where a further disclosure of information is needed to remedy the wrongdoing;
> 4) feedback on progress and completion to the individual who has raised the concern as far as is reasonably possible.[1254]

26. *Public Disclosures:* It is in the public interest to strike a balance between the exposure of wrongdoing to external bodies and the need for the Government to keep information confidential for national security reasons. The Tshwane Principles have balanced these interests by providing a list of factors that the individual will need to satisfy in order to obtain legal protection; these tests need to be satisfied on top of the tests outlined above. The tests that need to be satisfied as described in the Tshwane principles for an external disclosure are as follows:

[1251] Principle 39 of the Tshwane Principles, p.g.50.
[1252] Our advice is that all whistleblowing arrangements should follow best practice as stipulated by the Whistleblowing Commission's Code of Practice, p.g.28. http://www.pcaw.org.uk/files/WBC%20Report%20Final.pdf
[1253] This recommendation also follows of the Tshwane Principles, p.g.50.
[1254] Principle 39 C. of the Tshwane Principles, p.g.51.

(1) The person made a disclosure of the same or substantially similar information internally and/or to an independent oversight body and:
(i) the body to which the disclosure was made refused or failed to investigate the disclosure effectively, in accordance with applicable international standards; or
(ii) the person did not receive a reasonable and appropriate outcome within a reasonable and legally-defined period of time.
OR
(2) The person reasonably believed that there was a significant risk that making the disclosure internally and/or to an independent oversight body would have resulted in the destruction or concealment of evidence, interference with a witness, or retaliation against the person or a third party;
OR
(3) There was no established internal body or independent oversight body to which a disclosure could have been made;
OR
(4) The disclosure related to an act or omission that constituted a serious and imminent risk of danger to the life, health, and safety of persons, or to the environment.
AND
(b) The person making the disclosure only disclosed the amount of information that was reasonably necessary to bring to light the wrongdoing;
Note: If, in the process of disclosing information showing wrongdoing, a person also discloses documents that are not relevant to showing wrongdoing, the person should nonetheless be protected from retaliation unless the harm from disclosure outweighs any public interest in disclosure.
AND
(c) The person making the disclosure reasonably believed that the public interest in having the information revealed outweighed any harm to the public interest that would result from disclosure.

Note: The "reasonably believed" test is a mixed objective-subjective test. The person must actually have held the belief (subjectively), and it must have been reasonable for him or her to have done so (objectively). If contested, the person may need to defend the reasonableness of his or her belief and it is ultimately for an independent court or tribunal to determine whether this test has been satisfied so as to qualify the disclosure for protection.'[1255]

Grounds, Motivation and Proof

27. An individual should not forfeit protection for raising concerns where they are either incorrect about the wrongdoing they seek to raise, or where they have questionable motives for wanting to come forward. Protection should be forfeited only where an individual provided false information.[1256]

[1255] Ibid P.g. 51-52
[1256] Ibid p.g. 49

28. Connected to this point is that an individual should not have to provide evidence to justify the concern they are raising. Requiring evidence undercuts the chief aim of a whistleblowing framework which is to provide a safe space for individuals to raise concerns at the earliest opportunity to ensure incidents of wrongdoing or malpractice do not develop into situations that are more serious.[1257]

Protection from victimisation for making a disclosure of information

29. Research has shown that victimisation of an individual who has raised a concern is not just a personal injustice for the individual but can deter others from raising future concerns.[1258] For this reason the DIPB should prohibit victimisation or retaliation where the individual has either raised a concern, or is suspected of raising a concern.[1259]

30. An individual who has followed the disclosure regime should not be subjected to:

    1) Criminal proceedings, including but not limited to prosecution for the disclosure of classified or otherwise confidential information.
    2) Civil proceedings related to the disclosure of classified or confidential information, including but not limited to claims of damages and defamation proceedings.[1260]

31. Prohibited forms of victimisation or retaliation can include, though should not be limited to, the following:

    > "(a) Administrative measures or punishments, including but not limited to: letters of reprimand, retaliatory investigations, demotion, transfer, reassignment of duties, failure to promote, termination of employment, actions likely or intended to damage a person's reputation, or suspension or revocation of a security clearance;
    > (b) Physical or emotional harm or harassment,
    > (c) Threats of any of the above
    > (d) Action taken against individuals other than the person making the disclosure may, in certain circumstances, constitute prohibited retaliation."[1261]

32. The Judicial Commissioners should have the power to investigate suspected incidents of victimisation and/or retaliation of intelligence service personnel who have raised concerns. The Commissioners should not need to have a complainant to action an investigation into suspected acts of retaliation or victimisation.

[1257] Ibid p.g. 49
[1258] P.g.8 The Whistleblowing Commission, 2013.
[1259] Ibid p.g.53
[1260] Ibid p.g.53
[1261] Ibid p.g.53

33. The Judicial Commissioner should have the power to offer redress to the individual where they are satisfied that victimisation has occurred. They should have the authority to require the intelligence service to:

    (i) Reinstate or redeploy a member of the intelligence service;
    (ii) Award compensation, loss of wages, loss of holiday benefits, travel expenses, payment of legal fees or any other reasonable cost or expense;
    (iii) Recommend disciplinary action to any intelligence service personnel who has been judged to have been responsible for victimisation of an individual who has made a qualifying disclosure;
    (iv) Take action to stop or preventive action to stop the intelligence services from committing acts of victimisation.

34. The parties subject to an investigation into acts of victimisation should be informed of the Judicial Commissioners decision in written form, and there should be system of appeal for all parties involved in the investigation.

35. The Judicial Commissioner should complete the investigation within a legally determined time limit, unless the Judicial Commissioner believes the investigation will take longer to complete.

Public Interest Defence for the UK intelligence community

36. The public interest is an imprecise notion so there is a need to define the public interest or to give examples of wrongdoing in order to provide clarity for those who have witnessed wrongdoing (as stated above with a clear list of examples of the types of disclosures of information that would be covered by the legal framework). It would be helpful if the DIPB also gave guidance as to what factors would tend to indicate that a disclosure of information was made in the public interest. That guidance might helpfully extend to providing examples of disclosures of information that would, and would not, generally be regarded as being in the public interest.

37. To reduce uncertainty in this area it would make sense for either the Judicial Commissioners or the Government to produce guidance as to what factors would tend to indicate that a disclosure of information was made in the public interest.

38. The Tshwane Principles provide some pointers on how to determine whether the public interest in disclosure outweighs the public interest in non-disclosure. This can be determined in light of:

    a) Whether the extent of the disclosure was reasonably necessary to disclose the information of public interest;
    b) the extent and risk of harm to the public interest caused by the disclosure;
    c) Whether the person had reasonable grounds to believe that the disclosure would be in the public interest;

d) Whether the person attempted to make a protected disclosure through internal procedures and/or to an independent oversight body, and/or to the public, in compliance with the procedures outlined in Principles 38-40; and
e) The existence of exigent circumstances justifying the disclosure.[1262]

Conclusion

39. When introducing the DIPB to the House of Commons in November, the Home Secretary described the bill as *"setting out a modern legal framework that brings together current powers in a clear and comprehensible way, with a new Bill that provides some of the strongest protections and safeguards anywhere in the democratic world, and an approach that sets new standards for openness, transparency and oversight."*[1263] Creating a robust whistleblowing framework for those who work in the intelligence services will follow these sentiments and will go some way to create a truly forward thinking accountability structure around the new powers being formulated in the legislation.

40. The DIPB presents an opportunity for the UK to show leadership by providing a system of whistleblower protection for those working in the intelligence services. The UK already has a well-regarded legal framework for non-national security related whistleblowing. Implementing these proposals will fulfil both the recommended *"Advanced Steps"* from the Open Government Partnership guide for whistleblowing protection, and the UN Special Rapporteur who recommended member states implement the Tshwane principles, making the UK's legal framework truly world leading.[1264]

41. These proposals also represent an opportunity to reduce the risk of wrongdoing or malpractice in the oversight mechanisms being formulated for the use of far reaching surveillance powers by the UK government and are an important check on those powers by allowing public personnel to be protected when they disclose information about the abuse of those powers.

42. External oversight is key for the framework to have credibility for both individuals looking to raise a concern, and for other stakeholders including elected representatives or members of the general public. This a difficult balance to strike, there is public interest both in information being withheld on the grounds of national security and the uncovering of illegal behaviour and practices. These proposals

[1262] Ibid p.g.55-56.
[1263] P.g. 1, the Draft Investigatory Powers Bill, 2015
[1264] Open Government Guide, Whistleblowing, 2015- http://www.opengovguide.com/topics/whistleblower-protection/ and *"Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression"* ,report from the United Nations, 8th September 2015, http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/361

attempt to balancing these two sometimes competing concepts, and in doing so attempt to create a more effective and robust accountability system for the intelligence services.

Annex 1 Public Interest Disclosures by Intelligence Service Personnel

This amendment has been drafted to be placed after section 170 of the DIPB.

170 Protected Disclosures

(1) In this act a "protected disclosure" means any disclosure of information by a member of the intelligence service, regardless of its classification, in accordance with section 170-174.
(2) A "protected disclosure" means any disclosure of information which may pertain to the wrongdoing that has occurred, is occurring or is likely to occur:

(a) criminal offenses;
(b) human rights violations;
(c) international humanitarian law violations;
(d) corruption;
(e) dangers to public health and safety;
(f) dangers to the environment;
(g) abuse of public office;
(h) miscarriages of justice;
(i) mismanagement or waste of resources;
(j) retaliation for disclosure of any of the above listed categories of wrongdoing; and (k) deliberate concealment of any matter falling into one of the above categories.

(3) For the disclosure of information, as defined by section 2, to be considered a "protected disclosure", the member of the intelligence service, needs to:

(i) Have reasonable grounds to believe that the disclosure of information tends to show wrongdoing that falls within one of the categories within subsection (2);
(ii) The disclosure complies with conditions set forth in section 170.
(iii) The member of the intelligence service has not knowingly made a false disclosure of information;
(iv) A person making a protected disclosure should not be required to produce supporting evidence or bear the burden of proof in relation to the "protected disclosure".

172 Internal Disclosures

(1) A protected disclosure is made in accordance with this section if a member of the intelligence service makes a disclosure to his or her employer.
(2) The intelligence service shall establish internal whistleblowing procedures and designated a named person to receive protected disclosures.

173 Disclosures to Independent Oversight Bodies

(1) A protected disclosure is made in accordance with this section if a member of the intelligence service makes a disclosure to either the:

(a) The Judicial Commissioner; or
(b) The Intelligence and Security Committee of Parliament.

(2) The Independent Oversight Bodies should when receiving disclosures of information from an intelligence service personnel:

(i) Investigate the disclosure and take prompt action with a view to resolving the matter, or, after having considered the matter and consulted the person making the disclosure, to refer it to a body that is authorised and competent to investigate;
(ii) Where requested protect the identity of the intelligence service personnel who seek to make the disclosure in a confidential way;
(iii) Anonymous disclosures of information should be considered on their merits;
(iv) Protect the information disclosed and the fact a disclosure has been made except to the extent that further disclosure of information is necessary to remedy the matter;
(v) Feedback to the person making the disclosure of the progress and completion of an investgiation and, as far as possible, the steps taken or recommendations made.

174 Public Disclosures

(1) A public disclosure of information is considered a protected disclosure if made in accordance with this section where:

(i) A disclosure of information is made in accordance with section 170;
(ii) The person made a disclosure of the same or substantially similar information internally or to an Independent Oversight Body and: 1) the body to which the disclosure was made refused to investigate the disclosure effectively; 2) the person did not receive a reasonable and appropriate outcome; OR
(iii) a member of the intelligence service reasonably believed that there was a significant risk that making the disclosure internally and/or to the Independent Oversight Bodies would have resulted in the destruction or concealment of evidence, interference with a witness or victimisation against the person or a third party; OR
(iv) there was no established internal body or Independent Oversight Body to which a disclosure could be made; OR
(v) the disclosure related to an act or omission that constituted a serious and imminent risk of danger to the life, health and safety of persons, or the environment and;
(vi) a member of the intelligence service in making the disclosure only disclosed the amount of information that was reasonably necessary to bring to the light the wrongdoing and;
(vii) If a member of the intelligence service when making a disclosure also discloses documents or information that are no relevant to showing

wrongdoing, the person should nonetheless be protected from victimisation, in accordance with section 170-176, unless:

a) non-disclosure of the information outweighs the public interest in making the disclosure and;
b) the member of the intelligence service reasonably believed that the public interest in revealing the information outweighs any harm to the public interest that would result from the disclosure.

175 Protection against Victimisation

1) The member of the intelligence service who has made a disclosure in accordance with section170-174 should not be subjected to:

   (i) the person making the disclosure had reasonable grounds to believe that the information disclosed tends to show wrongdoing that falls within one of the categories set out in section 170; and (ii) the disclosure complies with the conditions set forth in 172-174.

2) Victimisation is prohibited against any member of the intelligence service who has made, or has wrongly been identified as having made, or may make a disclosure in accordance with section 170-174.
3) Victimisation includes, but is not limited to, the following:

   (i) Disciplinary action or administrative measures that include: letters of reprimand, retaliatory investigations, demotion, transfer, reassignment of duties, failure to promote, termination of employment, actions likely or intended to damage a person's reputation, or suspension or revocation of a security clearance;
   (ii) Physical or emotional harm or harassment or;
   (iii) Threats of any of the above.
   (iv) Action taken against individuals other than intelligence service personnel making the disclosure may, in certain circumstances, constitute prohibited retaliation.

176 Investgiation of Victimisation

1) The Judicial Commissioner will have the power to investigate allegations of victimisation, or a threat of victimisation, relating to a protected disclosure as outlined in section 175.
2) The Judicial Commissioner will investigate a reported act or threat of victimisation when:

   (i) A member of the intelligence service reports a complaint of victimisation in accordance with section 175;OR
   (ii) When the Judicial Commissioner believes that there are reasons to investigate allegations of victimisation.

3) Where the Judicial Commissioner as instigated an investgiation in line with subsection 2, they have the power, where they judge appropriate, to instigate, but not limited to, the following actions:

    (v) reinstate or redeploy a member of the intelligence service;
    (vi) award compensation, loss of wages, loss of holiday benefits, travel expenses, payment of legal fees or any other reasonable cost or expense;
    (vii) recommend disciplinary action to any intelligence service personnel who has been judged to have been responsible for victimisation of an individual who has made a protected disclosure;
    (viii) take action to stop or prevent the intelligence services from committing acts of victimisation;

4) In executing these powers the Judicial Commissioner will make every effort to ensure the proceedings are fair and in accordance with due process standards.
5) The investigation will either be completed over a six week period, or the parties will be notified of how long the Judicial Commissioners believe it will take to complete the investgiation.
6) The Judicial Commissioner will notify the parties to the investigation of their decision in the form of a written report.
7) An appeal can be lodged against a decision made by the Judicial Commissioner by the parties subjected to that decision.

177 Public Interest Defence for Intelligence Service Personnel

1) If a member of the intelligence services is subject to criminal or civil sanction relating to making a disclosure made in accordance with section 170-174, which is not otherwise protected under section 175, then a public interest defence can be sort, where the disclosure outweighs the public interest in non-disclosure.
2) The court or tribunal in deciding whether the public interest defence should be applied should consider:

    (i) Whether it was reasonably necessary to make the disclosure in the public interest;
    (ii) the extent and risk of harm to the public interest caused by the disclosure;
    (iii) whether the person had reasonable grounds to believe that the disclosure would be in the public interest;
    (iv) whether the person attempted to make a protected disclosure through internal procedures and/or to an independent oversight body, and/or to the public, in compliance with the procedures outlined section 170; and
    (v) Whether there were exigent circumstances justifying the disclosure.

21 December 2015

Zara Rahman—written evidence (IPB0079)

British citizen, data + technology researcher.

1. The powers suggested through the proposed Investigatory Powers Bill are not necessary, because they are based on the principle that mass surveillance works to deter crime. Based on numerous studies and comprehensive research, I dispute this.

2. Given the basis of the Bill in engaging in mass surveillance, I also believe that the Bill is not legal; both the Court of Justice of the European Union and the European Court of Human Rights have said mass surveillance is illegal.

3. Practically speaking, the suggestions are not workable, because the idea of an Internet Connection Record makes no sense. UK's biggest telecoms confirmed the plan is unworkable. It also fundamentally threatens the safety of the Internet; bulk efforts to undermine encryption are risky, as our societies depend upon a robust internet.

4. Otherwise, there are some fundamental misunderstandings within the bill; for example, the distinction between "content" and "communications data" is meaningless: metadata is actually more revealing than content. Creating huge databases of valuable metadata brings with it huge risks, for black hat hackers, and foreign governments. Securing against those potential threats is difficult, if not impossible.

5. The current Investigatory Powers Bill includes notable scrutiny loopholes, in which once issued, a Warrant can be modified to include new targets without new review and oversight. Oversight of powerful institutions is an essential keystone of our democracy, and this Bill threatens to remove this.

6. I strongly believe that the bill threatens freedom of expression within the UK; individuals should be innocent until proven guilty. Creating an environment in which whole communities feel subject to mass surveillance is an entirely counterproductive strategy and indeed a threat to our democracy, limiting our freedom of speech.

21 December 2015

Hon Sir Bruce Robertson—written evidence (IPB0141)

New Zealand Commissioner for Security Warrants

I have read with interest the Draft Bill and the surrounding and supporting material. I note that the proposed arrangements will cover all state intrusions and interceptions. In New Zealand there are different regimes which apply to applications made by the police as opposed to those made by the SIS and the GCSB. In my many years as a High Court Judge, I not infrequently considered applications by the Police under the Misuse of Drugs legislation and in respect of other alleged criminal activity. That was entirely a judicial function and the process worked without problems. Any Judge of the High Court can consider such an application. There is no involvement of the Executive in this task. I refrain from any comment on the multi-agency approach which is being maintained in your proposal.

I restrict these comments to my current role as Commissioner of Security Warrants which, as I apprehend the situation, is unique. I deal only with applications by the two security services where the Minister and I work in tandem in the issuing of the initial authorisations.

My office is created under Section 5A of the New Zealand Security intelligence Service Act 1969 which currently relevantly provides:

5A Commissioner of Security Warrants

1. There is a Commissioner of Security Warrants.
2. The Commissioner is appointed by the Governor-General on the recommendation of the Prime Minister following consultation with the Leader of the Opposition.
3. No person may be appointed as the Commissioner unless that person has previously held office as a Judge of the High Court.
4. No person may at the same time hold office as Commissioner and as Inspector-General under the Inspector-General of Intelligence and Security Act 1996.
5. The functions of the Commissioner are—
    a) to advise the Minister on applications for domestic intelligence warrants:
    b) to consider with the Minister applications for domestic intelligence warrants:
    c) to deliberate with the Minister on applications for domestic intelligence warrants:
    d) to issue domestic intelligence warrants jointly with the Minister in accordance with section 4A:
    e) to consider advice, given to the Commissioner under section 4F(3), concerning approvals to enter certain places:
    f) after consulting the Minister, to give directions under section 4F(5) (which relates to directions not to proceed with, or to discontinue, interceptions or seizures of communications at certain places):
    g) to conduct reviews under section 56 of the Telecommunications (Interception Capability and Security) Act 2013 relating to significant network security risks.

Section 15B of the Government Communications Security Bureau Act 2003 currently relevantly provides:

15B Involvement of Commissioner of Security Warrants

1. An application for, and issue of, an interception warrant or access authorisation under section 15A must be made jointly to, and issued jointly by, the Minister and the Commissioner of Security Warrants if anything that may be done under the warrant or authorisation is for the purpose of intercepting the private communications of a New Zealand citizen or permanent resident of New Zealand under—
    a) section 8A; or
    b) section 8B, to the extent that intercepting the person's private communications under that section is not precluded by section 14.
2. For the purposes of subsection (1), section 15A applies—
    a) as if references to the Minister were references to the Minister and the Commissioner of Security Warrants; and
    b) with any other necessary modifications.
3. In this section, ***Commissioner of Security Warrants*** means the Commissioner of Security Warrants appointed under section 5A of the New Zealand Security Intelligence Service Act 1969.

What that all means in simple operational terms is that no warrant is issued for domestic intelligence activity except with my involvement and concurrence. Both the services adopt a very conservative and cautious approach and if there is any possibility of a domestic aspect arising I am involved. My contribution is solely at the point of authorisation. I have no responsibility in respect of the manner in which the warrant is utilised. The monitoring and auditing function is the responsibility of the Inspector General of Security Services and her not inconsiderable staff.

From my perspective the New Zealand model works because it recognises and responds to the practical realities. Ministers all operate under pressure with enormous work flows. It is inevitable that in making decisions, even as significant as these, Ministers will necessarily heavily rely on briefing by their staff. I have the time to read in depth the voluminous files which are created in support of an application. These are an essential part of the rigour, discipline and integrity of the operation. As and when necessary, or appropriate, I meet in person with the legal officers, and sometimes desk and field officers involved with a particular application as I assess need, proportionality, reasonableness, alternatives, and safeguards. It is not unknown for some tightening of the application to take place in this phase. Having been a Judge for 28 years, I am experienced in critically weighing evidence against a statutory framework. I am not slow in challenging proposals and suggesting variations.

I then meet with the Minister in person. We discuss and evaluate the application and when we are each satisfied that the warrant is appropriate we jointly authorise the issue. Questions as to the standard of review to be applied by a Judicial officer do not arise because the statutory framework is clear that both the Minister and the Commissioner are issuers. There is at the initial stage the strongest recognition that there are principled issues of law and policy in play. Having the most elaborate schemes to review and critique the case

for a warrant after it has been issued cannot compare with having a mechanism for ensuring that the proper legal standards are being adhered to before the warrant comes into existence.

You will see that the appointment is made by the Governor General on the recommendation of the Prime Minister following consultation with the leader of the Opposition. My predecessor Sir John Jeffries, a retired High Court Judge, held the office for 14 years. He was re-appointed by different Governments. I was appointed to the High Court in 1987, was President of the Law Commission 2001 to 2005 and was a Court of Appeal Judge until I took early retirement in 2010. Since then I have continued as President of the Court of Appeal of Vanuatu, been appointed as President of the Pitcairn Islands Court of Appeal and a member of the Qatar International Court. I Chair the NZ Sports Tribunal and the Online Media Standards Authority as well as having sundry community and charitable roles.

At the core of the New Zealand arrangement is the twin authorisation to catch the two aspects of the decision making, and the extent and depth of involvement by a single designated judicial officer.

I am very happy to elaborate on the framework and operation if required.

14 December 2015

Ms. Coleen Rowley—written evidence (IPB0058)

I worked as an FBI Agent investigating crimes, including organized crime and some acts of terrorism, in the United States from 1981 through 2004. From 1990 to 2003, I held the position of Division Legal Counsel in the Minneapolis FBI, responsible for legal and ethical training of FBI agents and police officers. During my FBI career I also worked for brief periods in Paris and Montreal conducting liaison with foreign police and intelligence agencies.[1265]

In August of 2001, FBI agents in Minneapolis arrested (highly suspicious) French Moroccan flight student Zacarias Moussaoui on a visa overstay. Although Moussaoui's Al Qaeda and Chechen terrorist connections were quickly discovered, documented and even briefed on August 23, 2001 all the way up to Director of Central Intelligence George Tenet, in charge of the entire US intelligence community, still not all the "dots were connected." It was not until after the 9-11 attacks, that conclusive evidence of Moussaoui's connection to the 9-11 plot was gained. I wrote a whistleblower memo for the Joint Intelligence Committee Inquiry to better expose what the pre 9-11 problems had been regarding that investigation and later testified to the Senate Judiciary Committee about related endemic problems facing the FBI. Minneapolis case agent Harry Samit later testified in Moussaoui's trial that FBI Headquarters personnel had been "criminally negligent." An Inspector General investigation was launched in response to my memo that uncovered some even greater FBI-CIA failures to "connect the dots." Based on these investigations, the 9-11 Commission Report later identified a series of pre 9-11 errors and numerous recommendations for improvement, many of them revolving around the lack of information sharing due to excessive secrecy and the intelligence community's compartmentalization. In many cases officials named as recipients on key intelligence memos and important communications claimed they could not recall ever having seen these memos. It was generally (and accurately) concluded that better sharing of information inside agencies, between agencies and with the public before 9-11 could have prevented or at least reduced the harm done on 9-11.[1266]

I retired in 2004 but from news accounts, it's clear that the underlying problems have not been remedied in U.S. government investigative and intelligence agencies. Officials are still not able to read or process the information they already have, they do not share key information appropriately and they don't always act on important information. On the other hand, government officials of both the U.S. and U.K. have made a whole series of different errors in launching their "war on terrorism"[1267] which has only served to ratchet up the number of terrorist attacks in the world and to inspire greater numbers of people all over the world to violence. By some counts based on US State Department data, terrorist events have increased by 6,500% what they were before 9-11.

There are, of course, a number of American politicians pointing to the San Bernardino shootings to argue that the US must now do away with the minor reforms that just went into effect via the USA Freedom Act, which marginally reined in the collection of billions of pieces of (mostly non-relevant) metadata on Americans. These politicians claim law enforcement was unable to nip the murder plot in the bud because of the minor changes to collection and

[1265] Full bio at http://www.huffingtonpost.com/coleen-rowley/
[1266] http://articles.latimes.com/2010/oct/15/opinion/la-oe-rowley-wikileaks-20101015
[1267] http://journals.fcla.edu/ijie/article/view/83547

storage of metadata. Yet it's been revealed that the San Bernardino shooters were planning this well before the Snowden revelations and the passage of the Freedom Act. As Antiwar.com writer Justin Raimondo writes, "At a time when the authorities were scooping up this data as a matter of course, they simply missed it. And the reason they missed it is because they were collecting *everything*, with no way to differentiate some teenage girl's text messages to her friends from a terrorist's communications with her co-conspirator husband-to-be."[1268]

This further confirms what I have been warning for some time, well before Snowden's disclosures. In an opinion piece for *The Guardian* in November 2014,[1269] I tried to explain how collecting more non-relevant data, i.e. "hay" has not proven effective but will always tend to be counter-productive:

> *… Almost no one now remembers the typical response of counter-terrorism agency officials when asked why, in the spring and summer of 2001 in the lead-up to 9/11, they had failed to read and share intelligence or take action when "the system was blinking red" (the actual title of chapter eight of the US's 9/11 commission's report) and when the US director of central intelligence and other counter-terrorism chiefs were said to have had "their hair on fire".*
>
> *The common refrain back then was that, pre 9/11, intelligence had been flowing so fast and furiously, it was like a fire hose, "and you can't get a sip from a fire hose". Intelligence such as the Phoenix memo – which warned in July 2001 that terrorist suspects had been in flight schools and urgently requested further investigation – went unread.*
>
> *Although "can't get a sip" was a somewhat honest excuse, it was undercut when the Bush administration, days after the attacks, secretly turned on their illegal "Presidential Surveillance Program" to collect more, by a factor of thousands, of the communications of innocent American citizens, as well as those of billions of people around the globe.*
>
> *So the "fire hose" turned into a tsunami of non-relevant data, flooding databases and watch lists. The CIA had only about 16 names on its terrorist watch list back in September 2001 and probably most were justified, but there's no way the million names reportedly now on the "terrorist identities datamart environment" list can be very accurate. The decision to elevate quantity over quality did nothing to increase accuracy, unblock intelligence stovepipes or prevent terrorist attacks.*
>
> *…as an FBI whistleblower and witness for several US official inquiries into 9/11 intelligence failures, I fear that terrorists will succeed in carrying out future attacks – not despite the massive collect-it-all, dragnet approach to intelligence implemented since 9/11, but because of it. This approach has made terrorist activity more difficult to spot and prevent…*
>
> *The fearful citizen may not realise how difficult it is to search and analyse content due to sheer volume. They want to believe in the magic of data-mining to somehow predict future criminal behaviour. If only more contractors are hired and more money is spent to increase monitoring, if only laws can be passed forcing internet companies to constantly surveil every post and kitten image, coded and uncoded, in a multitude*

[1268] http://original.antiwar.com/justin/2015/12/17/no-easy-answers/

[1269] http://www.theguardian.com/commentisfree/2014/nov/28/bigger-haystack-harder-terrorist-communication-future-attacks

of languages, for signs of danger, the Orwellian argument goes, we will find the enemies.
But the real purpose in the egregiously stupid push to assign Facebook the fool's errand of monitoring everything seems to be to spread the blame. Leaving aside the privacy implications, what people need to grasp is that this is the kind of security thinking that doesn't just fail to protect us, it makes us less safe.

19 December 2015

Peter Rush—written evidence (IPB0033)

1. The article below is new and by the well-known investigative journalist Duncan Campbell.

It is my submission that having read it through you should call Mr. Campbell as a witness.

The article is currently at
http://www.theregister.co.uk/2015/12/16/big_brother_born_ntac_gchq_mi5_mass_surveillance_data_slurping/

2. It appears that Parliament has been misled and that powers requested by the Investigatory Powers Bill are, in part, to legitimise what has already been taking place illegally for years. I think it important that members of the committee should hear evidence from Mr. Campbell on this matter.

3. I have no connection with Mr. Campbell.

17 December 2015

Matthew Ryder QC—written evidence (IPB0142)

I gave oral evidence before the Joint Committee on the Draft Investigatory Powers Bill ('the Committee') on Wednesday 16 December 2015. I had been asked to answer specific questions provided in advance, but the evidence could not be completed. I have now been asked to provide my answers in writing.

QUESTIONS

1. **Do the oversight mechanisms in the draft Bill satisfy the requirements of Article 8 of the European Convention on Human Rights?**

1.1 No. There are currently a number of cases, both in the UK courts and in ECtHR, alleging non-compliance with Article 8 ECHR under existing legislation. Much of the Draft Bill replicates the existing oversight mechanisms and therefore would be subject to similar criticism and potential litigation.

1.2 The question may be specifically aimed at whether the oversight mechanisms set out in Part 8 are sufficient. But whether those oversight mechanisms (e.g, the Commissioners, or the Codes of Practice) are sufficient to adequately supervise all the powers contained in the Draft Bill, cannot be meaningfully answered in general terms, or in the abstract. For example, oversight mechanisms that may be appropriate for targeted surveillance, may be inadequate in the context of bulk equipment interference. Similarly, a process of oversight suitable for some cases, may be inadequate in other circumstances where journalistic or other types of confidential information are being obtained.

1.3 Compliance with Article 8, and the need for appropriate safeguards in order to be *'in accordance with the law'*[1270] depends on viewing the entire framework of safeguards relevant to the specific interference in question. For example, the level of detail contained in the Code of Practice will determine the way oversight is conducted by Judicial Commissioners. It will also depend on how those oversight mechanisms are operated in practice, including how well resourced they are.

2 **What is the legal status of the Codes of Practice under RIPA? What do you expect to be contained in the Codes of Practice issued under this Bill?**

2.1 The Codes of Practice under RIPA provide important guidance. This, in turn, contributes to the overall framework by which the quality of the legal provisions (and the extent to which they contain adequate safeguards) can be assessed.

2.2 The legal status of the Codes of Practice under RIPA is set out at section 72 of RIPA. That indicates, at section 72(2), that breach of the Code of Practice does not, <u>of itself</u>, result in criminal or civil liability under RIPA. However, a failure to comply with the Code may result in powers being exercised in a way that is not *'in accordance with*

[1270] A requirement of Article 8(2) of ECHR.

the law' for the purposes of Article 8 ECHR. It may also have other legal consequences such as the exclusion of evidence that might otherwise be admissible.

2.3 Furthermore, an inadequate code of practice, in the context of a surveillance regime, may contribute to a finding that the regime, taken as a whole, is in breach of Article 8 ECHR.[1271]

2.4 The question is very broad in its scope and it is not possible to set out in the limited time and space available everything that I would expect to be contained in Codes of Practice under the Draft Bill. However, and merely by way of example, I would expect new Codes of Practice to indicate appropriate protection for legal professional privilege, and protection of material of the kind that would fall within Schedule 1 of the Police and Criminal Evidence Act 1984, including a requirement of prior judicial authorisation.[1272] Further, I would expect new Codes of Practice to give clear guidance on the level of detail and specificity required in applications for warrants. The Codes of Practice should also provide clear guidance on the interpretation of relevant safeguards[1273] and their application. The Codes should also indicate the nature of any rules relating to the examination, retention and sharing of collected intercepted material, communications data and equipment data. This would include the extent to which data can be retained for different purposes than that for which it was obtained, as well as strict regulation on the retention of data for the purposes of intelligence databases.

2.5 Further, I am aware of the answer to this question provided by Mr Martin Chamberlain QC, and agree with his observations.

3 What practical effect is the introduction of a right of appeal from the Investigatory Powers Tribunal likely to have?

3.1 This will enable an appeal to the Court of Appeal on points of law. It brings the Investigatory Powers Tribunal in line with other Courts that deal with serious infringements of fundamental rights, and allows an appeal to a panel of highly experienced, senior judges. In this regard, I respectfully agree with the observations of David Anderson QC on this topic, in his report *'A Question of Trust'* at paragraph 14.105 and recommendation 114.

3.2 Consistent with Mr Anderson's recommendation, clause 180(1), amends RIPA by inserting a new section 67A, which indicates that an appeal may lie on a 'point of law'. However, the new section 67A(4) suggests that the Court of Appeal may not grant leave to appeal *'unless it considers that –(a) the appeal would raise an important point of principle or practice, or (b) there is another compelling reason for granting leave.'*

[1271] See, for example, *Liberty v UK* (2009) 48 EHRR 1; or the consideration of the codes of practice in *Gillan and Quinton v UK* (2010) EHRR 45, in relation to the interference with Article 8 through a stop and search power,
[1272] As distinct form judicial 'approval' under judicial review principles.
[1273] For example, those at clauses 40-41; 103; 117-120; 146 -148;

3.3 I do not believe section 67A(4) is suitably drafted. There is a danger that such a provision might be interpreted to require the Court of Appeal to refuse leave to appeal, even if it considers there are arguable grounds that the Investigatory Powers Tribunal made a significant error of law, merely because that error does not also engage an 'important point of principle and practice'. This would be unconscionable and allow identified errors of law to be without remedy on appeal. As a result the proposed section 67A(4) of RIPA is, at best, unhelpful. It is either misguided, because it directs that leave should be refused in some cases even though a significant error of law may have been made by the IPT, merely because the case does not involve 'an important point of principle or practice'. Alternatively, it is irrelevant, because it will always be interpreted as permitting leave to be granted whenever a significant error of law may have been made, on the basis that this would be a 'compelling reason' for granting leave.

3.4 In the circumstances, I suggest consideration should be given to amending clause 180 and removing or amending the proposed section 67A(4) of RIPA. Consideration should be given to a clause that would be closer to the usual test for permission in the Court of Appeal on a point of law.[1274]

4 **Why is it important that the Investigatory Powers Tribunal is able to hold as much of its proceedings in public as possible**?

4.1 The IPT performs the function of a court through which persons may seek legal remedies for infringements of their fundamental rights. It is a well-established principle of open justice that a court performing such a function should hold as much of its proceedings in public as is possible. [1275] This principle is subject to established qualifications, relating both to the rights of privacy of the parties and witnesses, but also to considerations such as national security or other reasons why some or all of a hearing cannot be held in public. But the fundamental presumption in favour of open justice remains and applies to the IPT.

4.2 Public hearings, where possible, are recognised by the IPT as an important part of discharging its oversight function.[1276] It is a positive development that public hearings in the IPT are now more common than in the past. In all cases, particularly those challenging the Government's interpretation of statutory provisions and the proper ambit of surveillance powers, open hearings and judgments are a crucial element of public confidence in the entire surveillance system. I would not support any suggestion of reducing the IPT's ability to hold public hearings. I would also welcome any effort to ensure a greater commitment to having the IPT's work made available to the public insofar as is possible. In particular, any blanket prohibition on publicity

[1274] See CPR 52.6: 'Permission to appeal may be given only where – (a0 the course considers that the appeal would have a real prospect of success; or (b) there is some other compelling reason why the appeal should be heard.'
[1275] For recent discussions on the principles of open justice, R (Guardian News and Media) v City of Westminster Magistrates Court and others [2012] EWCA Civ 42. paragraph 69 onwards; and R (BSkyB) v Commissioner of Police for the Metropolis [2014] UKSC 17
[1276] In the Matter of Application Nos IPT/01/62 and IPT/01/77, 23 January 2003

of categories of IPT judgments (e.g. an absolute ban on providing any details of a finding against a complainant) is undesirable and should be reconsidered.[1277]

4.3 Further, I am aware of the answer to this question provided by Mr Martin Chamberlain QC, and agree with his observations.

5 Is it appropriate that material acquired from targeted equipment interference warrants may be used as evidence in legal proceedings? Is it desirable?

5.1 It is appropriate and desirable. It is consistent with the well-established presumption, that relevant evidence should be admissible in legal proceedings. There are, of course, some equally well-established exceptions that rebut that presumption (e.g. evidence that may be subject to legal professional privilege, or evidence that has been obtained through torture). There are also instances where even though evidence may be admissible, a trial judge has a discretion to exclude it on the basis, for example, that it would be unfair for the evidence to be adduced in evidence.

5.2 I have considered this issue further, in answer to question 12, below.

6 Is there an on-going justification for intercept material remaining inadmissible in legal proceedings?

6.1 I am not persuaded that such a justification exists. The most recent explanation for the rule, (currently contained in section 17 of RIPA; and in clause 42 of the Draft Bill) is set out in the final report of the *'Intercept as Evidence Review'*,[1278] chaired by Sir John Chilcot. That final report was published in December 2014. In contrast, I consider the points raised in the highly praised report by Justice in 2006, entitled, *'Lifting the Ban',*[1279] to be compelling. That detailed report explained the shortcomings of the rule and the lack of apparent justification for it: http://bit.ly/1Yw2npH.

7 The Bill creates a new offence of disclosing the fact that warrants for equipment interference have been authorised and that such activities have taken place (Clause 102). Will this have any impact on legal proceedings in your view?

7.1 This question overlaps with the issues in question 12, which I have considered in more detail, below.

7.2 A separate, narrower point also arises under this question. That is to do with companies, organisations or individuals who are directly affected by such an offence (e.g. telecommunications operator) including those who may have professional reasons why they wish to disclose the nature of equipment interference for important reasons in the public interest. There will need to be greater guidance as to

[1277] See, for example, the provisions relating to rulings against a complainant, RIPA section 68(4), being limited to no more than a statement that he or she has been unsuccessful.
[1278] http://bit.ly/1QUtYQG
[1279] http://bit.ly/1Yw2npH

what will constitute the 'reasonable excuse' defence, for such persons and organisations.

7.3 I understand several organisations affected by this provision have made submissions on this aspect of the Draft Bill, and I defer to their submissions on this point without adding my own.

8 **Is the retention of data for 12 months a proportionate balance between the needs of the security services and law enforcement and the rights of the individual?**

8.1 I understand that several organisations and individuals have made submissions to the Committee on this point. They include those who have been party to on-going litigation over the retention of communications data, as well as those directly affected by any legal requirement to retain it. They are better placed to comment on the propriety of a requirement for retention of 12 months and I defer to those submissions.

9 **Does clause 13(2) meet common law and ECHR requirements as to the detail to be included in warrants and is it sufficiently clear in its terms, for example in explaining what is meant by group etc. or does it require significant amendment if it is to remain in the Bill?**

9.1 It does not. Clause 13(2) provides no meaningful guidance on the detail that must be included in a warrant. It simply indicates that a warrant may target a person, an organisation, or anything else falling within clause 13(2). It does not indicate the level of detail and specificity required in such warrants.

9.2 This is significant omission in the Draft Bill. Unless there is clarity as to the level of focus and specificity required in a warrant a number of problems arise:

- The person applying for the warrant does not know how much detail they need to provide; neither does the Secretary of State or the judicial officer know how much detail is required before authorising or approving an application. It potentially permits applications for warrants to be drafted and granted on broad, general terms, giving far reaching discretion to those carrying out activity under those warrants.

- Unlike search warrant cases under section 8 or Schedule 1 of PACE where the warrant is subsequently disclosed to the affected person after its execution, the person affected by warrants issued pursuant to powers in the Draft Bill will remain in the dark. Therefore a person who might seek to challenge the lawfulness of a warrant based on its lack of specificity, will not be in a position to do so. In order to protect that person's fundamental rights, greater specificity is required to determine what should be set out in the warrant and at what level of detail.

- Without better clarification as to what detail is required, there is a real risk that clause 13(2) may be interpreted to permit *'thematic warrants'* i.e. warrants based not on the identity of known individuals, or the identity of a known group of individuals, but on a theme relating to general activity by persons unknown (e.g. all persons within a city who may be committing activity of a certain description). Such an interpretation transforms what are presented as domestic 'targeted' interception warrants into warrants that permit general surveillance in the hope of determining who, amongst potentially millions of people, might be engaged in the activity in question. This amounts to a significant shift from existing English law principles relating to the interference of the state with an individual's private possessions or communications. It can only be avoided and/or properly regulated by greater specificity as to what level of detail is required in a warrant, and what may properly be authorised. If, as many have submitted to this Committee, thematic warrants should not be permitted, this should be made clear in the Bill and in Codes of Practice.

10 **Should the present powers relating to bulk interception warrants be replicated in the draft Bill or should warrants be more narrowly focused as to their purpose and permitted search criteria?**

10.1 I do not think the existing powers should be replicated in the Draft Bill, and I believe that warrants should be more narrowly focused. I am currently leading counsel in litigation before ECtHR[1280] on this and associated points. For reasons stated in that application, it is my view that the present powers relating to bulk interception warrants are unlawful and in breach of Article 8 and Article 10 ECHR. I am strengthened in that view by the very recent decision of the ECtHR.: *Zakharov v Russia* [2015] ECHR 1065.

Although the Agencies have long claimed the power to hack - carry out equipment interference under the Intelligence Services Act - police now unambiguously have that power as well - the amendment of s 10 Computer Misuse Act 1990 by s 44 of the Serious Crime Act 2015. Prior to that they were limited to physical actions analogous to the planting of bugs as "Property Interference" under the Police Act 1997 and an associated Code of Practice. Now they can plant and use back doors to enter computers, retrieve password to other computers and activate device microphones and cameras. At the moment the draft Equipment Interference Code of Practice appears to be limited to actions by the SIAs.

11 **Are the proposals in the Draft Bill at s 89 (sic) and following adequate to deal with the range of intrusions that are possible? Are you concerned about the current lack of an associated draft Code of Practice?**

11.1 Insofar as the police use of equipment interference is concerned, I do not consider the current provisions sufficient. Equipment interference is potentially extremely damaging not only to the hardware and software of persons and networks subjected to it, but to public trust and confidence in the integrity and privacy of our networks

[1280] *10 Human Rights Organisations v UK* Application No. 24960/15, communicated on 30 November 2015

and devices. It should require an application by an officer at a very senior level, and should not be permitted without prior judicial authorisation.

11.2 Further, a more detailed code of practice is necessary.

11.3 I have one additional recommendation in relation to the authorisation of equipment interference. In relation to all applications for warrants relating to equipment interference it is my opinion that there should be thorough consideration to the risk of unintended consequences arising out of the proposed interference. This may include the risks created by the alteration of software, planting of malware, or the accessing of hardware. Such activity is not properly analogous to physical actions historically covered by 'property interference', such as entering property and planting bugging devices. Equipment interference (which includes 'computer network exploitation') can be akin to disrupting and permanently altering the proper execution of computer code and the safe use of trusted networks, as well as the reliability of widely used and commercially available software. The unintended consequences of such interference, include the risk of disrupting and corrupting national and transnational networks, as well as undermining public confidence in commercial devices and products. For that reason, I believe serious consideration should be given to an enhanced advisory committee that can give informed technical expert advice, both to those applying for warrants as well as those authorising and approving them, in order to properly understand the risks of such activity. It is another reason why equipment interference should be significantly constrained and more limited in relation to its potential use.

11.4 I am aware that several others who have made submissions to this Committee, including Liberty and Privacy International, have addressed concerns on these issues and defer to those submissions without repeating them.

12 **Section 102 creates an offence of unauthorised disclosure of equipment interference warrants. What impact could this have to the disclosure obligations under the Criminal Procedure and Investigations Act 1996? What is your opinion of the hypothesis that defendants will routinely allege hostile equipment interference on their computers and smart phones by law enforcement and that defence lawyers will then seek to have such evidence excluded for unreliability and potential contamination under s 78 PACE?**

12.1 This issue is of some significance and would require a more detailed explanation than is possible in the time and space permitted. There are a number of important points.

12.2 First, there appears to be no equivalent of section 17 of RIPA or clause 42 of the Draft Bill applicable to Part V of the Draft Bill. This means that, under Clause 102, the Draft Bill contemplates a criminal offence of disclosure of the existence of a Part V warrant, subject to a 'reasonable excuse' defence. But – unlike intercept material - the product of a Part V warrant is *potentially*[1281] admissible in legal proceedings. Further

[1281] Highly sensitive material may be admissible, even though it would only be in highly exceptional cases that it would be disclosed or used in evidence (e.g. the identity of a police informant).

clarification would be helpful. In particular, there should be guidance on the circumstances that might constitute a 'reasonable excuse' to the offence under Clause 102 (e.g. disclosure to a judge in ex parte proceedings; disclosure on order from a judge; etc.). That guidance should be in the form of additional statutory provisions as well as codes of practice and/or prosecutorial guidance.

12.3 Second, in order to understand the consequences of how this may impact on criminal proceedings it is important to consider the relevant principles of disclosure:

- The Criminal Procedure and Investigations Act 1996 requires disclosure to a defendant of all relevant material that might undermine the prosecution or assist the defence.[1282] That disclosure obligation is a fundamental requirement of a fair trial.[1283] The disclosure requirement applies even if the material in question would not be admissible in evidence.

- Accordingly, even if the prosecution is not adducing material derived from an equipment interference warrant in evidence, the prosecution may need to disclose its existence and the existence of the warrant under which it was derived. Clause 102 will therefore need to be amended or clarified to ensure such disclosure is not a criminal offence.

- Significantly, such disclosure may be relevant to enable a defendant to mount a challenge to the integrity of the evidence being presented in the case against him or her (e.g. evidence from a computer or phone that may have been affected, corrupted or made unreliable by the method of equipment interference). If, for reasons of operational sensitivity or otherwise a prosecutor was not able to make such disclosure, the prosecution would have to be abandoned: a prosecution would be in breach of Article 6 ECHR (the right to a fair trial) if the prosecution proceeded without making disclosures to the defendant pursuant to relevant disclosure obligations.

- It is possible that a cynical defendant may seek to exploit this position and suggest the existence of an equipment interference warrant will always need to be disclosed in order for the defendant to be able to make submissions on the integrity of the evidence. The defendant's hope may be that the time, expense or sensitivity involved in such disclosure may cause the prosecution to have to be abandoned. However, criminal courts are well experienced in distinguishing between requests for disclosure that are speculative 'fishing expeditions' designed merely to disrupt a prosecution, and those which are genuine requests for the disclosure of relevant material.

- Nevertheless, widespread use of equipment interference, in this context, would be likely to cause significant disclosure problems. The prosecutor may not even be in a position to know how a particular form of equipment

[1282] See section 3 of that Act.
[1283] See *R v H* [2004] UKHL 3

interference might have affected the integrity of other evidence in the case. Similarly, the prosecutor may not be able to conclude, with confidence, whether or not such disclosure was unnecessary in order for the defendant to have a fair trial. A trial judge would be unlikely to be able to provide any further assistance or technical insight for the prosecutor. Accordingly, in many instances the prosecution would either have to err on the side of caution and make such disclosure, or abandon the prosecution.

- While similar problems necessarily arise in relation to the blanket ban on intercept material under section 17 of RIPA (replicated clause 42 of the Draft Bill), these problems are likely to be more far-reaching in the context of equipment interference. This is because equipment interference, unlike interception, is more likely to have wider technical implications on the integrity of other evidence.

- In order to overcome these problems, a prosecutor would need to be clear on the technical implications of the equipment interference in question; the likely affect it has on the reliability of associated evidence; and would need to have access to expert advice on any potential arguments that may be advanced by the defence. Where necessary, the prosecutor would need to be able to disclose the existence of the Part V warrant and how the equipment interference occurred, in order to ensure that the defence was given adequate disclosure and the prosecution did not have to be abandoned. The above measures would mitigate, to some degree, the difficulties caused by the prosecutor's disclosure obligations in the context of equipment interference warrants. Conversely, widespread, highly sensitive and unpredictable use of equipment interference - both in bulk and in targeted form - would be likely to cause a prosecutor significant problems in properly discharging disclosure duties. This, in turn would result in significant disclosures having to be made to defendants and/or otherwise meritorious prosecutions having to be abandoned. It is another reason why equipment interference, where it is permitted, should be tightly constrained and more closely regulated than it currently is under the Draft Bill.

22 December 2015

Scottish PEN—written evidence (IPB0076)

We are making this statement in the capacity of Scottish PEN, the Scottish centre of the world association of writers, PEN International. It is a charitable body for the advancement of the education of the public by the following means: i) The encouragement and promotion of writing in and about Scotland nationally and internationally; ii) The support of writers worldwide in the interest of freedom and artistic expression; iii) The fostering of international understanding through the appreciation of literature; iv) The attendance of Scottish PEN representatives at conferences, symposia and other meetings of writers worldwide; v) The organisation in Scotland of conferences and other literary events; vi) The undertaking of any legal activity to further these charitable objects provided that Scottish PEN shall in no circumstances engage in political activities.

INTRODUCTION

1. As an organisation charged with representing writers to ensure the fundamental freedoms to write, read and share thoughts, there are a number of aspects of the draft Investigatory Powers Bill that could threaten these freedoms were they to be made into law.

2. We have polled our membership of over 300 writers, including fiction, non-fiction, journalists and poets for their reactions to the enhanced surveillance proposals contained within the draft bill. The answers of the 22 respondents have informed this submission. The polling questions can be found in APPENDIX I (31-34)

3. Further to the supplying answers to the questionnaire, Scottish PEN members were given the opportunity to present a statement in relation to the draft Investigatory Powers Bill (named or anonymous) these can be found in APPENDIX II (35-47)

4. The three aspects within the bill that we are focusing on relate directly to the freedom of our membership and the broader writing community within Scotland to write and read. These aspects are: (1) the retention of Internet Connection Records (ICRs) by telecommunications providers of every British citizen for 12 months that can be accessed by public bodies; (2) Technical Capabilities Notices, that can give the Home Secretary increased capacity to pass on obligations to telecommunication providers. This is widely held to contain the obligation to build in backdoors to online communications platforms for the security services to collect user data, as well as the ability to decrypt data on demand; and (3) the prevalence of gag orders that restrict knowledge of the actions contained within the draft bill being shared with journalists, customers and the wider community. This can include the aforementioned technical capabilities notices (s.189); interception (s.43 (1-7)); equipment interference (s.148); and retaining communications data (s.77).

INTERNET CONNECTION RECORDS (ICR)

5. The draft bill stipulates an obligation of telecommunications providers to hold for 12 months the ICRs of every British citizen for 12 months that can be accessed by public

bodies without a warrant. This contains everything in a URL prior to the first forward slash.

6. While this to protect against capturing 'content', many commentators and technical experts questions the ability to effectively make this distinction.

7. Scottish PEN is deeply concerned about how this will enable the state and the security services to construct remote profiles of Internet users from their browsing history alone.

8. Scottish PEN represents writers and readers who, at times, research and read challenging material that represents a broad and diverse set of values that do not at any given time fully or accurately represent their own personally held political, social or religious beliefs.

9. Earlier this year, PEN International commissioned a study into the impact of mass surveillance on writers around the world. "The survey findings demonstrate that increasing levels of surveillance in democracies are seriously damaging freedom of expression and thought, the free flow of information, and creative freedom around the world."[1284]

10. These findings supported the findings of the PEN American Center who commissioned a similar study of US based writers in 2013 who found that "1 in 6 writers has avoided writing or speaking on a topic they thought would subject them to surveillance" [1285]

11. In the polling of Scottish PEN members, over half of respondents answered that the retention of ICRs will change how they conduct their research and source information online.

12. Encouraging writers and readers to engage in self-censorship to 'escape' surveillance cannot ensure the free expression that defines a modern democracy.

13. Writers, readers and researchers require privacy to ensure they can complete their work free from undue attention or pressure that may hinder their freedom in fully exploring the issues they are focusing on.

14. Requiring public bodies to seek approval through a communications data acquisition notice and not a warrant signed by a judge removes a much-needed level of oversight to ensure that they are independently judged to be acting in a "necessary and proportionate" manner. While the designated person is required to be independent from the investigative team requesting the notice, the fact that they are

[1284]PEN INTERNATIONAL, 01/05/2015-last update, *Global Chilling: The Impact of Mass Surveillance on International Writers*. Available: https://www.pen.org/sites/default/files/globalchilling_2015.pdf [20/12/2015].
[1285]PEN AMERICAN CENTER, 2014-last update, *Chilling Effects: NSA Surveillance Drives Writers to Self-Censor*. Available: http://www.pen-international.org/read-pen-american-centres-report-chilling-effects-nsa-surveillance-drives-writers-to-self-censor/ [20/12/2015].

representing the same body raises key questions as to whether this amounts to independent scrutiny.

15. Writers in Scotland have already experienced the dangers of unclear or vague oversight procedures through the highly publicised issue of Police Scotland 'committing "multiple breaches" of a new code intended to guard against unlawful spying on journalists'[1286] which, at the time of writing, is currently being investigating by the Interception of Communications Commissioner's Office (IOCCO).

TECHNICAL CAPABILITIES NOTICES

16. Section 189 (1) stipulates, "the Secretary of State may make regulations imposing specified obligations on relevant operators, or relevant operators of a specified description."

17. We are concerned about the vague nature of this section as it does not specify the limits to these actions, going on to state that "Regulations under this section may impose an obligation on any relevant operators only if the Secretary of State considers it is reasonable to do so."

18. Technical experts such as Glynn Moody at Ars Technica and George Danezis, an associate professor in security and privacy engineering at University College London have stated that this section may be used to empower telecommunications providers to build in backdoors in their software for the security services and decrypt data on demand.

19. Further clarification is necessary to ensure that all actions that are contained within this section fully compile with all existing legislation.

20. Backdoors in online platforms weaken the overall security of the platform opening up users to vulnerabilities that can be exploited by hackers and other third parties. This concern has been vocalised by Tim Cook, the CEO of Apple, who stated that: "You can't have a back door in the software because you can't have a back door that's only for the good guys," [1287]

21. This is of utmost importance to a wide range of writers in Scotland who require secure communications platforms to ensure they can communicate with a wide range of individuals and organisations including publishers, editors, agents and magazines.

22. Assuming that the creation of backdoors into telecommunications services is included within s.189, 55% of Scottish PEN members who responded to the

[1286]HALL, K., 2015. *Police Scotland fingered for breaching RIPA code 'multiple' times*. http://www.theregister.co.uk/2015/09/21/police_scotland_broke_ripa_code_whistleblower_witchhunt_ban/ edn. The Register.

[1287]NEWCOMER, E., 2015. *Apple CEO Defends Encryption, Opposes Government Back Door.* http://www.bloomberg.com/news/articles/2015-10-20/apple-ceo-defends-encryption-opposes-government-back-door edn. Bloomberg.

questionnaire responded that they would not continue to use a platform that had been compromised by the state.

23. Further to this, over 60% of all respondents claimed that this infiltration of key services would either *somewhat affect* or *seriously affect* their communications with *colleagues in the UK (63.4%); colleagues abroad (81%); friends & family (82%).*

24. The commercial importance of manuscripts and early drafts cannot be undervalued. As a result the intellectual property of the writers can be undermined if the security of the online platforms they use to communicate cannot be guaranteed.

GAG NOTICES

25. Throughout the draft bill are a range of gag orders that restrict the ability of telecommunications providers, customers, journalists and civil society from being made aware of a number of the aspects contained within the bill.

26. Glynn Moody and George Danezis have identified these notices throughout the bill: "interception (Section 43(1-7)); "equipment interference" (hacking—Section 148); and retaining communications data (Section 77). Gag orders would also be in place for bulk communications data collection (Section 133)."[1288]

27. Scottish PEN condemns any actions that limit the free flow of information, restrict understanding and undermine debate on key issues surrounding freedom of expression.

28. The inability of telecommunications providers to communicate actions carried out as part of this draft legislation makes it impossible for customers, including writers, readers and researchers, to make an informed decision as to whether to continue to use platforms that may have been compromised by the security services.

29. These notices are punishable by up to 12 months imprisonment and/or fines and Scottish PEN is deeply concerned that the severity of these punishments will dissuade whistle-blowers and further limit the flow of information to the public.

30. In the questionnaire to Scottish PEN members, respondents reacted to this breach of trust in a manner that significantly undermines their relationship with the state. When asked whether the inability of telecommunications providers or journalists to share information surrounding key aspects of the draft bill affected their trust of key bodies, 77% of respondents stated that they would *severely distrust* the UK government, 68% answered the same in regards to telecommunications providers and 59% said that they would *severely distrust* writers and journalists as a result of their inability to report accurately on the contents of the draft bill.

[1288]MOODY, G., 2015. *Snooper's Charter: UK gov't can demand backdoors, give prison sentences for disclosing them*. http://arstechnica.co.uk/tech-policy/2015/11/snoopers-charter-uk-govt-can-demand-backdoors-give-prison-sentences-for-disclosing-them/ edn. Ars Technica.

ANNEX I: Questionnaire to Scottish PEN Members

31. The draft Investigatory Powers Bill includes a legal obligation of telecommunications services to hold Internet Connection Records of every British citizen for 12 month to be accessed by public bodies without a warrant. Will this change how you conduct your research and source information online?

    Yes
    No
    Other

32. If a platform that you use on a regular basis (such as social media platforms, emails, online shopping, banking...) had been compromised by the intelligence agencies, would you continue to use it?

    Yes
    No
    Not sure
    Other

33. If your email platform had been compromised by the intelligence agencies, would this affect your communication with the following individuals or groups?

    Publishers:

    Colleagues in the UK:

    Colleagues abroad:

    Friends & Family:

34. If the government was able to access private services (such as social media platforms, emails, online shopping, banking...) and journalists and the telecommunication providers themselves were unable to openly share information about this, how would this affect your trust in the following services?

    UK Government:

    Press & Journalists:

    Service Providers:

APPENDIX II: Written Statements from Scottish PEN Members

35. I am for the highest degree of openness and transparency compatible with safeguarding security. Public acknowledgment in due course by service providers of such intrusions should therefore be normal. –Professor Richard H. Roberts

36. It is must be inferred that the encroachments proposed by the current government on public and private media, services, platforms and providers will do little to combat organized crime or terrorism. Any such offender with a smidgen of nous, and surely that means most, will keep abreast of developments of this kind and take appropriate measures to ensure safe passage and unobserved action. As the present government acts to reduce the range and volume of the state, layer by layer, what parts of it remain will become increasingly vulnerable to access by corporate interest, in other words by global companies whose command of advanced technology will eclipse anything the intelligence services, dependent on relatively small state budgets, will be able to muster. As that fulcrum is reached, all data previously encrypted by government services, as well as data the present government wishes to access and more, will be available for exploitation, including sell-on to interested parties. Not only the current capabilities and practices of specialized hackers but also the political history of our own era post-1933 already show that it is essential for the public to take special care to protect its data and ultimately personal safety as well as the existence of civil society in all its remaining forms against the actions of future (at present unimagined) governments, state and military agencies, and corporate interest. The present government believes it needs more information to fight our enemies. In fact, the opposite is true: the more information generated and retained, the more vulnerable our societies become. –Iain Galbraith

37. I oppose any measures designed to limit the level of confidentiality between providers and users such as the Internet Connection Record. The test of reasonableness would need strict definition. My opposition applies to proposed measures emanating from both Westminster and Holyrood. –Anonymous

38. Anyone who assumes privacy in cyberspace is a fool. It's all compromised already. No I am not paranoid. I am a Computer Science academic. Anything digital can be seamlessly copied and transmitted. There is no encryption that can't be broken. Really. If you need secrecy use the postal services. It takes far more human effort to open and read a letter than to scan a digital artefact. And after a letter is destroyed it can't be copied. When you delete email what has actually been deleted? And from where? –Anonymous

39. As I understand them, the provisions are so loosely defined that they invite abuse. The assumption that everyone has to be watched is very disturbing. –Anonymous

40. I think it compromises citizens' rights to free speech, free interchange of ideas, and private communication. I don't want to live under surveillance, and I don't believe it ultimately makes anyone any safer. –Anonymous

41. The Bill is like using a sledgehammer to crack a marshmallow. –Anonymous

42. The Bill extends powers to the State which are not obviously different from those in regimes recognised as repressive and are of a piece with current government encouragement to eg teachers to report 'subversive' activity or views among their pupils. Of course the state needs to protect its citizens but it is arguable that sufficient means to do that exist already. For instance the identities of the ringleaders of the recent Paris attacks were apparently known to the international police and the problem was a failure to act on information not a failure of surveillance. A key consideration with me is that however apparently benign the intention in setting up further and far-reaching means of surveillance, once such mechanisms are set up and accepted it is easy for them to be misused. It could be the first step to the UK becoming a police state. –Anonymous

43. This doesn't significantly change my view of the state nor will it significantly alter my behaviours. I have nothing to hide and know that openness is the best policy. I'm sure they would find most of my communications boring. –Anonymous

44. This change to the law represents a major intrusion into civil liberties, and a huge addition to the powers of surveillance by the state. A writer's thoughts and the ways he/she has to generate new work - and also the way he/she communicates, and who with - must be kept private in order to produce the work. I completely oppose this bill. –Anonymous

45. I am very concerned about the undemocratic and sweeping nature of the powers this bill suggests. I am also extremely concerned about the appalling short time for its consideration. –Anonymous

46. It's an infringement of civil liberties, taking us back to feudal times. –Anonymous

47. Targeted investigatory powers are essential in some cases but it is "overkill" to introduce such elastic and invasive powers for everyone. –A Connolly

21 December 2015

Serious Fraud Office—written evidence (IPB0153)

Summary

I. The Serious Fraud Office (SFO) is the independent government department which investigates and, where appropriate, prosecutes cases of serious or complex fraud as set out in the Criminal Justice Act 1987.

II. The SFO welcomes this Bill. Investigatory powers to obtain communications data are essential, and their use is increasing in the SFO's work.

III. The SFO would resist any future requirement for it to enter into a collaboration agreement for the authorisation of access to communications data because the SFO considers that being required to enter such an agreement would adversely affect its ability to investigate and prosecute serious fraud, bribery and corruption.

IV. The Bill could be used to amend an anomaly in existing legislation whereby some of the SFO's investigatory powers apply only to corruption offences, and not to other types of fraud.

Introduction

1. The Serious Fraud Office (SFO) welcomes the Bill but has concerns about its potential impact on the way the SFO obtains communications data.

2. In the time available, this written evidence focuses on the likely effect the Bill would have on the work of the SFO. Where we are able to answer questions from this perspective, we do so below.

3. The role of the SFO is to help protect 'UK Plc' and society from the top-most tier of serious or complex fraud, which includes international bribery, corruption and related money laundering.

4. The SFO investigates and (if appropriate) prosecutes those who commit serious or complex fraud. It also pursues offenders to recover the financial proceeds of their crimes. It has the power to investigate and prosecute corporate bodies, as well as individuals.

5. The Director of the SFO is superintended by the Attorney General. The Attorney General and other law officers speak for the Government on matters relating to the SFO in the Houses of Parliament.

6. Examples of the SFO's current caseload include investigations relating to the manipulation of the 'LIBOR' rate, Rolls Royce, Tesco, GlaxoSmithKline, Barclays, GPT/Sangcom and G4S/Serco. SFO investigations can often involve the UK's biggest companies – household names. They are high profile, high risk investigations, in which many people may have an interest. It is essential that the SFO's work, both investigatory and prosecutorial, can be carried out without interference. Independence is an important safeguard for the SFO: the Directors' decisions have been challenged in the courts, and independence is essential for maintaining the confidence of the public and of non-Government organisations which operate in this area. Information held by the SFO is extremely commercially sensitive. Any reporting of the SFO's involvement with a publicly listed company has to be properly handled through the correct channels.

7. The SFO has unique statutory powers, which can be used to compel others to provide information under section 2 of the Criminal Justice Act 1987 (but not communications data). The SFO uses its powers to obtain communications data under existing law (RIPA). Communications data is important to investigating complex international fraud conspiracies and as evidence for use in its prosecutions. It is important in uncovering criminality, and helping to direct and focus investigatory activity.

8. Investigatory powers to retain and acquire communications data are essential to advance investigations into serious and complex economic crime and for use as

evidence in court. The use of devices and online activity to facilitate and perpetuate illicit activity has increased rapidly. As a consequence, the acquisition of communications data, and the identification of services to which individuals or devices have connected, are vital to combat serious fraud and there has been exponential growth in the SFO's acquisition of such data.

9. The frequency with which the SFO has obtained communications data has increased substantially over recent years, and is expected to continue increasing. Applications have increased by 75% in the last year, and more than trebled since 2013. Reasons for this include the increasing use of such e-technology by suspects, and the SFO's increasing capability to tackle 'crime in action' (rather than simply reacting to reports of historic crime).

10. The SFO's increased capability to investigate crime happening in real time means that the SFO is better placed now to investigate crimes currently in progress, rather than relying on reports after a crime has taken place. This allows the SFO to acquire evidence at an earlier stage and thus reduce the time taken for investigations and prosecutions, and from the time that the crime occurs to a resolution in the criminal justice system. It also provides opportunities for more and better evidence to be collected for prosecutions because there is less elapsed time for it to be altered, moved or destroyed.

11. In order to maintain and develop our investigative capability, we need to keep up to date with the range of technologies used to commit serious economic crimes. The SFO therefore welcomes the provisions which would enable it to continue authorising its own applications for communications data, subject to the stated safeguards. The law must be kept under constant review to ensure it keeps pace with technology and its use.

12. Access must be proportionate: bearing in mind individuals' rights to privacy, the usefulness of such material to investigators, and the seriousness of the relevant criminality.

Responses to the Committee's specific questions

Overarching/thematic questions:

Are the powers sought necessary? Has the case been made, both for the new powers and for the restated and clarified existing powers?

13. The power to obtain communications data is an essential investigation tool for SFO.

14. Ensuring that communications service providers (CSPs) retain communications data, and that it can be obtained by SFO with necessary safeguards, would help us to maintain our capability in line with current and technological developments. Because of their complexity, SFO cases can typically take several years from start to finish, so the SFO favours longer retention periods for communications data.

Are the powers sought legal? Are the powers compatible with the Human Rights Act and the ECHR? Is the requirement that they be exercised only when necessary and proportionate fully addressed? Are they sufficiently clear and accessible on the face of the draft Bill? Is the legal framework such that CSPs (especially those based abroad) will be persuaded to comply? Are concerns around accessing journalists', legally privileged and MPs' communications sufficiently addressed?

15. The Serious Fraud Office has no comments on this question.

Are the powers sought workable and carefully defined? Are the technological definitions accurate and meaningful (e.g. content vs communications data, internet connection records etc.)? Does the draft Bill adequately explain the types of activity that could be undertaken under these powers? Is the wording of the powers sustainable in the light of rapidly evolving technologies and user behaviours? Overall is the Bill future-proofed as it stands?

16. In respect of the obtaining and retention of communications data, the powers are sufficiently defined and workable for the SFO (except regarding clause 63 as described from paragraph 44 onwards below).

Are the powers sought sufficiently supervised? Is the authorisation process appropriate? Will the oversight bodies be able adequately to scrutinise their operation? What ability will Parliament and the public have to check and raise concerns about the use of these powers?

17. The Serious Fraud Office has no comments on this question (except regarding clause 63 as described from paragraph 44 onwards below).

Specific questions:

General

To what extent is it necessary for (a) the security and intelligence services and (b) law enforcement to have access to investigatory powers such as those contained in the Draft Investigatory Powers Bill?

18. Please see paragraphs 8-15 above.

Are there any additional investigatory powers that security and intelligence services or law enforcement agencies should have which are not included in the draft Bill?

19. There is an inconsistency in the current legislation which means that some of the SFO's powers can be applied to certain bribery and corruption cases only, and not to other types of fraud case.

20. Section 2 of the Criminal Justice Act 1987 (the Act) gives the Director of the SFO power to compel relevant individuals to produce documents, attend interview and answer questions or otherwise furnish for the purposes of an investigation under section 1(3) of the Act. This section provides that "The Director may investigate any

suspected offence which appears to him on reasonable grounds to involve serious or complex fraud."

21. An amendment to section 2A of the Act was later introduced[1289] allowing the powers of the Director under section 2 to be exercisable for the purpose of enabling him to determine whether to start an investigation in a case involving overseas bribery and corruption offences where it appears that an offence *may have* been committed. This means that the SFO can investigate matters of overseas bribery and corruption and use its section 2 powers at an earlier stage, when the evidential picture is less developed.

22. There is therefore now a discrepancy between the types of powers available under the Act: the SFO has greater powers where the alleged offence is overseas bribery or corruption than it does where the alleged offence is domestic serious fraud.

23. Without the ability to compel the production of relevant financial information at an early stage, the SFO has to rely on other sources which may not be as productive. For instance, reports by regulators which take time to complete and are compiled for a different purpose.

24. Information gathered in other ways can take longer to obtain which introduces delay and, in turn, often attracts criticism. This may enable a fraud to be perpetrated over a longer period of time, involving more victims or greater losses; or allow evidence to be destroyed or removed.

25. In criminal investigations, the standard of proof is 'beyond reasonable doubt'. For regulatory matters, there is a lower threshold and so correspondingly information is obtained and used for different purposes and may not always meet the evidential standard for criminal prosecution.

[1289] Criminal Justice and Immigration Act 2008 s59

26. These powers also augment the SFO's ability to threaten crime which is current. This is an important tool for the SFO, as it is for other investigators. With the advent of Deferred Prosecution Agreements (DPA) in the UK, it is also an essential part of encouraging corporates to use these new provisions.

27. DPAs may be entered into only by the Director of Public Prosecutions or the Director of the SFO, with the agreement of the Courts. Amending the law to enable the SFO to conduct pre-investigatory enquiries for all types of offence that it prosecutes would also help to support the DPA regime by better demonstrating to companies the importance of making a self-report.

28. This bill would be suitable for remedying the current anomaly. The SFO has case studies and other information available about this issue which it would be happy to supply to the Committee.

Are the new offences proposed in the draft Bill necessary? Are the suggested punishments appropriate?

29. The Serious Fraud Office has no comments on this question.

Interception

Are there sufficient operational justifications for undertaking (a) targeted and (b) bulk interception?

30. The Serious Fraud Office has no comments on this question.

Are the proposed authorisation processes for such interception activities appropriate? Is the proposed process for authorising urgent warrants workable?

31. The Serious Fraud Office has no comments on this question.

Are the proposed safeguards sufficient for the secure retention of material obtained from interception?

32. The Serious Fraud Office has no comments on this question.

How well does the current process under Mutual Legal Assistance Treaties (MLATs) work for the acquisition of communications data? What will be the effect of the extra-territorial application of the provisions on communications data in the draft Bill?

33. The arrangements to acquire material through Mutual Legal Assistance are critical to investigations and prosecutions in the UK and overseas. It is a vital tool in combating fraud, bribery and corruption which is international in nature. The SFO supports the separate work that is underway to improve the processes under the existing UK/US Treaty to obtain communications data.

34. The effect of the extraterritorial application of the provisions in the Bill is necessary to maintain the continued access of law enforcement to communications data and content. The SFO supports this.

Communications Data

Are the definitions of content and communications data (including the distinction between 'entities' and 'events') sufficiently clear and practical for the purposes of accessing such data?

35. Yes, the bill needs to be technology neutral in order to stand the test of time. Redefining communications data, a complex area into two categories of 'entity' and 'events' data achieves this aim. The new definitions are clear and practical and the publication of draft Codes of Practice to accompany the bill will assist in explaining how the new definitions will work in practice.

Does the draft Bill allow the appropriate organisations, and people within those organisations, access to communications data?

36. The Serious Fraud Office has no comments on this question.

Are there sufficient operational justifications for accessing communications data in bulk?

37. The Serious Fraud Office has no comments on this question.

Is the authorisation process for accessing communications data appropriate?

38. The SFO recognises that the overall authorisation process is necessary and proportionate to what is sought to be achieved.

39. However, clause 63 of the Bill gives the Secretary of State authority to direct that agencies enter collaboration agreements. This power could be exercised to apply to any public authority, including the SFO.

40. Under this provision, public authorities which access communications data could be required to go through a shared Single Point of Contact (SPoC) (suggestions include making use of the National Anti-Fraud Network). This is not the preferred authorisation process for the SFO because of the need to protect confidentiality and operational security of our investigations.

41. The Bill also provides judicial authorisation for all applications to access communications data for the purposes of identifying or confirming the identity of journalist's source. Currently, this must be obtained using an order from a judge under the Police and Criminal Evidence Act 1984. The SFO currently does not have the power to seek such an order in its own right so it is important to make this change and amend this inconsistency.

Data Retention

Do the proposed authorisation regime and safeguards for bulk data retention meet the requirements set out in the CJEU Digital Rights Ireland and the Court of Appeal Davis judgments?

42. The Serious Fraud Office has no comments on this question.

Is accessing Internet Connection Records essential for the purposes of IP resolution and identifying of persons of interest? Are there alternative mechanisms? Are the proposed safeguards on accessing Internet Connection Records data appropriate?

43. The Serious Fraud Office has no comments on this question.

Are the requirements placed on service providers necessary and feasible?

44. The Serious Fraud Office has no comments on this question.

Equipment Interference

Should the security and intelligence services have access to powers to undertake (a) targeted and (b) bulk equipment interference? Should law enforcement also have access to such powers?

45. The Serious Fraud Office has no comments on this question.

Are the authorisation processes for such equipment interference activities appropriate?

46. The Serious Fraud Office has no comments on this question.

Are the safeguards for such activities sufficient?

47. The Serious Fraud Office has no comments on this question.

Bulk Personal Data

Is the use of bulk personal datasets by the security and intelligence services appropriate? Are the safeguards sufficient for the retention and access of potentially highly sensitive data?

48. The Serious Fraud Office has no comments on this question.

Oversight

What are the advantages and disadvantages of the proposed creation of a single Judicial Commission to oversee the use of investigatory powers?

49. The SFO welcomes the proposal to reduce the number of reporting bodies. There are clearly efficiencies that can be made by public authorities who are monitored if reporting to only one body instead of two.

Would the proposed Judicial Commission have sufficient powers, resources and independence to perform its role satisfactorily?

50. The Serious Fraud Office has no comments on this question.

Are the appointment and accountability arrangements for Judicial Commissioners appropriate?

51. The Serious Fraud Office has no comments on this question.

Are the new arrangements for the Investigatory Powers Tribunal including the possibility of appeal adequate or are further changes necessary?

52. The Serious Fraud Office has no comments on this question.

Conclusion

53. The SFO welcomes the Bill which is essential to maintain a position where law enforcement agencies are able to use communications data as part of investigations and prosecutions. Without these powers which currently exist, the ability of agencies to combat serious crime would be significantly diminished.

54. The SFO remains concerned that a requirement to enter a collaboration agreement to obtain communications data would undermine the SFO's unique role in the law enforcement landscape. In recommending the creation of a single body to investigate and prosecute serious fraud cases, the report of the Fraud Trials Committee, which was chaired by Lord Roskill, says at paragraph 2.46

> "Such an organisation with unified control and direction would have a number of distinct advantages. In particular, fewer serious frauds would be allowed to escape prosecution by slipping through the net of a series of independent organisations working in this field; overlapping of resources could be avoided; it would enable the investigation process to lead to more effective prosecution; there would be scope for greater efficiency and the reduction of delays; unhelpful restrictions on the disclosure of information from one organisation to another would be avoided, and a unified organisation would have full powers of investigations."

55. Every one of these identified benefits would be undermined by a requirement for the SFO to seek communications data through a third party.

6 January 2016

Graham Smith—supplementary written evidence (IPB0126)

ABOUT THE AUTHOR

1. I am a solicitor in practice in London. My legal expertise is primarily in the fields of IT, the internet and intellectual property. I am the editor and main author of the textbook Internet Law and Regulation, first published in 1996 (4th edition 2007, Sweet & Maxwell).

2. I have advised private sector clients on RIPA from time to time since its inception. I contributed to the discussion of DRIPA during its rapid passage through Parliament, primarily through an analysis of the draft DRIP Bill posted on my Cyberleagle blog. I made a submission to the Anderson Review (https://app.box.com/s/84t7w7b91ebstrn7qvvu1xoqrb5gb2r6).

3. This submission is made in my personal capacity. It should not be taken as representing the view of any client for whom I have acted or of Bird & Bird LLP, the firm in which I am a partner.

4. I have also submitted evidence to the House of Commons Science and Technology Committee[1290], which I incorporate by reference.

5. I have set out below only those selected questions (in the general Call for Evidence and also specific questions indicated for my Oral Evidence session) to which I am providing a response. These represent only a small proportion of the issues raised by the draft Bill. For the most part I have concentrated on issues around clarity and scope of powers rather than debating the merits or otherwise of policies implemented in the draft Bill.

RESPONSE TO GENERAL CALL FOR EVIDENCE

A. OVERARCHING/THEMATIC QUESTIONS

ARE THE POWERS SOUGHT WORKABLE AND CAREFULLY DEFINED?

- **ARE THE TECHNOLOGICAL DEFINITIONS ACCURATE AND MEANINGFUL (E.G. CONTENT VS COMMUNICATIONS DATA, INTERNET CONNECTION RECORDS ETC.)?**

6. As will be seen from my responses to specific questions below, in some places there are significant problems with lack of clarity of definitions.

7. In some places (especially Internet Connection Records) critical terms that are not common currency or terms of art have been left undefined, leading to significant uncertainty as to their scope.

8. The Committee has heard evidence of the difficulty that the industry has had in correlating the definitions with actual datatypes held in, processed by or transmitted through their systems. If industry is experiencing difficulty, can the general public

1290 http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25119.pdf.

foresee with any degree of certainty the kinds of data that may be subject to retention, acquisition, interception or examination?

9. Definitions such as '"Data" includes any information which is not data' surely invite comparisons with the impenetrability of RIPA.

- **DOES THE DRAFT BILL ADEQUATELY EXPLAIN THE TYPES OF ACTIVITY THAT COULD BE UNDERTAKEN UNDER THESE POWERS?**

10. The draft Bill is certainly a significant improvement on RIPA. For instance the arrangement whereby bulk interception warrants are set out in a separate section headed 'Bulk interception warrants' is far preferable to the reader having to hack through the impenetrable jungle of RIPA, chance upon Sections 8(4) and 16 and then have the insight to perceive that 'certificated warrants' are about bulk interception. The draft Bill is quite logically set out and it is generally explicit about the types of powers that it would grant.

11. However the draft Bill retains some of RIPA's vices. In respect of powers, chief among these is the obscurity of the apparently wide power to collect and examine related communications data as a by-product of bulk interception. In RIPA the potential extent of this power is revealed by chaining together collateral powers: metaphorically navigating the back alleys of the statute. For interception that arrangement has effectively been transposed into the draft Bill. (See further, response to Oral Evidence Question 16.)

12. The draft Bill also introduces some new problems of its own. These derive mainly from the definitional issues already mentioned. The definitions and intersections of various types of data – communications data, relevant communications data, related communications data, contents of a communication and so on – are difficult to conceptualise. The only realistic way to understand them is to test a list of real world examples against them and see which fall on which side of the various lines. The Home Office accompanying documents give a few examples, but not enough to test the definitions fully.

13. The Home Office could usefully produce a comprehensive list of datatype examples, where appropriate with explanations of context, categorised as to whether the Home Office believes that each would be entity data, events data, contents of a communication, data capable of being related communications data when extracted from the contents of a communication and so on.

14. A schedule of this type would inform the debate on this aspect of the draft Bill immeasurably. (In case it is of interest to the Committee, the batch of Snowden documents published by The Intercept in September 2015 contains an example of such a document.[1291])

1291 https://theintercept.com/document/2015/09/25/content-metadata-matrix/

15. Codes of Practice can helpfully include non-controversial illustrations of datatypes. However for reasons explained in my response to Oral Evidence Question 10 that is no substitute for a well formulated and intelligible statutory provision.

Undefined terms

16. Clause 47(4) uses the terms 'internet service' and 'internet communications service'. Neither term is defined.

17. Presumably 'internet communications service' is intended to be narrower than 'internet service'. However the draft Bill gives no indication as to where the dividing line between them may be. 'Internet service' does not appear to have previously been used in UK primary legislation. 'Internet access service', a more readily understandable term, has been used previously in both the Digital Economy Act 2010 and DRIPA.

18. 'Internet communications service' was used in DRIPA, where it was also undefined[1292]. That lack of definition may be because DRIPA replicated the 2009 Data Retention Regulations, which implemented the (now invalidated) EU Data Retention Directive. The Directive used the term 'internet communications service' but itself did not define it (see http://cyberleagle.blogspot.co.uk/2014/12/another-round-of-data-retention.html). It is not a term of art.

19. The Explanatory Note at para 120 refers to: "Identifying which communication services a person has been using, for example determining whether they are communicating through apps on their phone." The implication may be that an "internet communications service" is intended to be restricted to messaging services – i.e. services by which human beings send each other messages (as opposed to, for instance, submitting search requests to a search engine) and to exclude automated device to server (or server to device) communication such as a software or data update.

20. That impression is reinforced by para 122 of the Explanatory Note: "In respect of purposes b. and c., the designated senior officer within a relevant public authority could only approve the application if it was to determine how *an individual has been communicating with another individual online*…".

21. However paragraph 46 of the Guide to Powers and Safeguards refers to using ICRs to identify "services a suspect has accessed which could help in an investigation including, for example, mapping services". The only clause 47 gateway that appears to be relevant to the example is 47(4)(b). That would not permit access to an ICR unless a mapping service were an 'internet communications service'. That would give the term much wider scope than human to human messaging. If that is the intention, we have no clarity as to the actual width of 'internet communications service' or how it might differ from an 'internet service'.

[1292] The current Data Retention Code of Practice attempts to provide an explanation. It says: "An internet communications service under DRIPA as amended by the CTSA is a communications service which takes place on the internet and can include internet telephony, internet email and instant messaging services."

22. If, on the other hand, 'internet communications service' is intended to be limited to human to human messaging, the draft Bill does not make that clear. Nor, if that is intended, are we told how activities such as human to human messaging within online gaming services would be approached.

23. The meanings of 'internet service' and 'internet communications service' and the intended dividing line between them ought to be explained and articulated in the legislation.

- **IS THE WORDING OF THE POWERS SUSTAINABLE IN THE LIGHT OF RAPIDLY EVOLVING TECHNOLOGIES AND USER BEHAVIOURS?**

24. See next comments on future-proofing.

- **OVERALL IS THE BILL FUTURE-PROOFED AS IT STANDS?**

25. Future-proofing has two sides. They are in tension with each other.

26. The first is to protect the powers against changes in technology, so that they are not rendered ineffective by new technologies falling outside the text of the legislation. Future-proofing in this sense leads to technology neutral drafting, which while gaining in terms of longevity tends to be abstract, difficult to understand and unclear as to how it applies to real world activities.

27. The second side to future-proofing is to ensure that the balance between intrusiveness and privacy settled upon by Parliament when it passes legislation of this kind is not thrown out of kilter by advances in technology. As technology reaches further into people's lives, so technology-neutral powers will automatically follow. As the powers start to apply to unanticipated types of behaviour the consequences may be quite different from those envisaged by Parliament when it passed the legislation.

28. That has happened with RIPA. The combination of internet and mobile phone technology has, by a mere accident of technology, caught within RIPA's net an ever-growing swathe of everyday activities and consequently thrown an avalanche of new data into the hands of law enforcement and the intelligence agencies. While the powers have remained the same, the balance between privacy and intrusion now embodied in RIPA bears little resemblance to that settled upon by Parliament in 2000. In that sense RIPA was anything but future-proofed.

29. Future-proofing of the second kind leans in the opposite direction from future-proofing of powers. It tends towards concrete, technology-specific drafting (and thus greater intelligibility), sunsetting of powers and frequent revisiting by Parliament (a) to ensure that the intended balance is maintained and (b) to consider any request to plug any gaps in powers that may have appeared.

30. Such a process also requires continuing information and openness about how the powers have been used, so that Parliament may engage in an informed debate when it comes to review the legislation[1293].

31. Overall the draft Bill attempts to future-proof in the first sense, with predictable consequences of some very widely drawn powers and some relatively abstract and complex definitions. In my personal view the RIPA experience should teach us that this is undesirable and that the greater need is to future-proof whatever balance between intrusion and privacy Parliament decides to settle upon.

B. SPECIFIC QUESTIONS:

COMMUNICATIONS DATA

- **ARE THE DEFINITIONS OF CONTENT AND COMMUNICATIONS DATA (INCLUDING THE DISTINCTION BETWEEN 'ENTITIES' AND 'EVENTS') SUFFICIENTLY CLEAR AND PRACTICAL FOR THE PURPOSES OF ACCESSING SUCH DATA?**

'Content of a communication' compared with RIPA.

32. RIPA has no definition of the content(s) of a communication. The meaning of 'content' underpins in RIPA (and will do under the draft Bill) not just the distinction between content and communications data for the purposes of warrants, data retention and acquisition notices, but also the scope of the interception offence and other provisions of the draft Bill. The clauses in which 'content of the communication' occurs include:

    3(1)(b), 3(5): definition of interception

    12(8), 106(8): extraction of related communications data from content of a communication (similarly 82(4) in relation to equipment interference, using similar definition of content in 82(8); and similarly 136(4) and 136(8); cf 149(2))

    16(1): protection for MPs

    33(2): lawful authority for interception by telecommunications service providers

    45(1): definition of intercepted material

    119(4): restrictions on examination of bulk intercepted material (both nature of material and purpose); similarly 147(4) for bulk equipment interference

    121(1): definition of intercepted material

    193(5): definition of communications data

[1293] In that regard the various new non-disclosure provisions in the draft Bill give cause for concern. For instance the Home Office has publicly stated that the Clause 71 powers will be used to mandate the retention (or creation) of ICRs. However, as discussed in my oral evidence Clause 71 is far wider than that. If the use of Clause 71 were to be extended beyond ICRs in the future there appears to be no requirement on the Home Office to bring that to the attention of the public or Parliament, either before or after the event. Service providers would be bound not to reveal the content of the data retention notices by means of which such a change of policy was implemented.

33. The scope of the interception offence under RIPA has been the source of considerable uncertainty (see paragraphs 66 to 75 of my submission to the Anderson Review). Against such a fuzzy baseline it is difficult to say whether the new definition of content results in something much the same, broader or narrower.

34. However there are indications that it may be narrower. Chief among these is the omission from the draft Bill of any equivalent, for telecommunications, of S.2(5) RIPA.

35. S.2(5) provides that for both postal and telecommunications services interception does not include "conduct that takes place in relation only to so much of the communication as consists in traffic data comprised in … a communication … for the purposes of any … telecommunication system by means of which it is or may be transmitted".

36. The draft Bill retains a corresponding provision for postal communications (for which no new definition of content is provided), but not for telecommunications. It may be that the new definition of content has narrowed the scope of interception sufficiently to render a saving for accessing traffic data superfluous. This may be the result of clause 196(6)(a) (see discussion at paras 46 to 47 below).

The definition of 'content of a communication'

37. The framers of the draft Bill have the challenge of devising a definition that works as well for machine to machine communications as it does for person to person e-mails and messages.

38. This is a relevant consideration even without considering developments such as the internet of things. For instance when we access a website a series of background communications takes place between our web browser and the website server. Those messages are structured according to the HTTP protocol, with various sections and subsections. We have to be able to determine which of those sections contain content and which (if any) contain communications data (or, under the draft Bill's provisions for related communications data, contain data that would not be content when separated from the rest of the message).

39. The main part of the definition revolves around the 'meaning of the communication'. If I send an e-mail, does this definition encompass only the message that I have composed and sent? Or does it also include the elements of that communication that mean something to the computers that will process them?

40. If the former, then large parts of most communications would not be content. Some parts might not be communications data either.

41. The latter seems more appropriate and likely, given the ubiquity of background machine to machine communications. However the definition then drives us to ask "For a computer to computer communication, what is the meaning of 'meaning'?". Whether that is a good outcome deserves further consideration.

42. The definition of content is couched in terms of "what might reasonably be expected to be" the meaning of the communication. Crudely, if it looks like content, it is. If it doesn't, it is not.

43. Thus the definition is framed from the perspective of the potential interceptor or retainer or acquirer of data, rather than from the perspective of the person whose communication it is. This is presumably intended to provide comfort to those making decisions about what type of authority is required to access the information.

Content, interception and data retention

44. The data retention provisions in Part 4 of the draft Bill do not, unlike the communications data acquisitions provisions of Part 3, exclude acts of interception from conduct that a data retention notice may require. On the other hand Clause 5(1) does not include data retention notices in the list of provisions that amount to lawful authority for interception.

45. Yet it seems that in order to create ICRs service providers may have to perform some interception-like activities in order to extract from transmissions some kinds of destination data (e.g. names of services).

46. Clause 193(6)(a) appears to prevent such activity being interception by excluding from content 'anything in the context of web browsing which identifies the telecommunications service concerned'.

47. On the one hand this is highly technology-specific. It does not address any situations outside the context of web browsing (for instance a service accessed using a mobile app). On the other hand it excludes such data from content for all purposes in the draft Bill (see list in para 32 above).

Conclusion on definitions of content and communications data

48. The new definitions of content and communications data will fall to be applied within a wide variety of contexts.

49. It is difficult to propose alternative formulations without fully understanding what the Home Office intends should be the result of applying the definitions.

50. Given the significance of the definitions and the potential uncertainties about how they might apply it would be of considerable assistance if the Home Office were to produce a comprehensive list of examples as suggested above (paras 12 to 14).

DATA RETENTION

- **IS ACCESSING INTERNET CONNECTION RECORDS ESSENTIAL FOR THE PURPOSES OF IP RESOLUTION AND IDENTIFYING OF PERSONS OF INTEREST? ARE THERE ALTERNATIVE MECHANISMS? ARE THE PROPOSED SAFEGUARDS ON ACCESSING INTERNET CONNECTION RECORDS DATA APPROPRIATE?**

51. My comments are of necessity limited to a few impressions from reading the Operational Case for the Retention of ICRs without either specialist technical knowledge or operational expertise.

52. For Purpose 1 the Operational Case suggests that it is 'likely' that the matching process will identify a particular device as it is 'unlikely' that 'many, if any' of the other 5,000 devices using that IP address were accessing that email website in the same minute. (page 10).

53. The usefulness of this process appears to depend on the extent of the reduction that would be achieved by the matching process. A process that reduced 5,000 users to 1,000 would, presumably, be of little assistance.

54. The Operational Case could helpfully have provided more detail as to why a useful degree of reduction would be 'likely' as opposed to, say, a hope or possibility. The Committee has heard evidence about devices remaining continuously connected to particular services in order to receive notifications.

55. The Operational Case does not refer to the Danish experience of session logging, as to which written evidence has been provided to the House of Commons Science and Technology Committee. If the Home Office is proposing a different approach that could be expected to yield better results than the Danish experience, the Operational Case could usefully have indicated what that approach is and why it holds out the prospect of better results.

OVERSIGHT

- **WOULD THE PROPOSED JUDICIAL COMMISSION HAVE SUFFICIENT POWERS, RESOURCES AND INDEPENDENCE TO PERFORM ITS ROLE SATISFACTORILY?**

56. See response to oral evidence Question 8.

RESPONSE TO ORAL EVIDENCE QUESTIONS

(ORIGINAL NUMBERING)

OVERVIEW

Q.1. ASIDE FROM THE NEW POWERS ON THE RETENTION OF INTERNET CONNECTION RECORDS, DOES THE DRAFT BILL CONSOLIDATE EXISTING POWERS OR DOES IT EXTEND THEM?

57. The draft Bill both consolidates existing powers and extends them. See my oral evidence and the detailed table in my evidence to the House Of Commons Science and Technology Committee.

58. In summary, leaving aside the question of whether explicit thematic, equipment interference and bulk data acquisition powers are or are not new:

Internet Connection Records

59. The additional communications data retention powers in Part 4 (clause 71) go far beyond Internet Connection Records, covering:

- Any type of human to human communication.
- Background activities of my smartphone when any app decides to communicate with a server – e.g. notification, data or software update.
- Any machine to machine communication – connected home thermostat, my car checking if it needs a software update, anything connected to the internet or any other network. In other words, the internet of things.

60. The above types of communication are all new compared with the current DRIPA schedule, which apart from internet access applies only to certain human to human messaging: internet e-mail, SMS messages and internet telephony. They also go beyond the amendments to DRIPA made by S.21 of the Counter-Terrorism and Security Act 2015 (IP address resolution)[1294].

61. Additionally:

- Inclusion of private services and systems is new (Cl.71(1) and 193(1)).
- The power in Clause 71 to require data to be generated for retention is new.
- The power in Clause 71 to require data to be obtained for retention is new (this point is additional to the points made in my oral evidence).
- The current limitation to retention of data generated or processed in the UK is removed.

Technical capability notices (Cl 189)

62. Under RIPA (S.12) and the 2002 Maintenance of Interception Capability Order made under it notices may be issued to certain public service providers in order to require a technical capability to support interception. Under the draft Bill:

- For interception, technical capability notices are extended to private operators.
- The powers to issue technical capability notices in support of the targeted, thematic and bulk warrants under Parts 5 and 6 are new.
- The power to issue technical capability notices in support of acquisition of communications data under Part 3 is new.

Bulk interception

[1294] The current Data Retention Code of Practice sets out at paragraph 2.14 a list of IP address resolution datatypes which is identical to Clause 71(9)(a) to (e) of the draft Bill. However the way in which the list is used in each case is different. In the Code the listed items are given as illustrations of types of data that might be necessary to identify the IP address used by the sender or recipient of a communication, i.e. for IP address resolution purposes. In Clause 71(9) of the draft Bill the list is used in a reverse sense. It is presented as a self-standing list of things that 'relevant' communications data should be capable of identifying or assisting in identifying. That is far broader in scope than the usage in the Code, even assuming that the items in the Code list are in fact capable of assisting in the identification of the device or person using an IP address, which for most of the items on the list is not obvious.

- A new power to treat some content as related communications data (108(8)).
- This is replicated for 'equipment data' in the new bulk acquisition and equipment interference powers

'Telecommunications operators'

- The use of this new, broad, definition has a knock-on effect of expanding targeted and bulk interception powers

63. See also my separate discussion above of the new definitions of content and communications data, including whether they may have the effect of narrowing the scope of 'interception'.

OVERSIGHT

Q.8. DO THE OVERSIGHT MECHANISMS IN THE DRAFT BILL SATISFY THE REQUIREMENTS OF ARTICLE 8 OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS?

64. Under this heading I raise the question of secret legal interpretations.

65. Where powers are exercised or asserted on the basis of interpretations of statutory powers that are not made known to the public, the question could arise whether the requirement that the law be accessible to the public is satisfied. In any event, in terms of establishing public trust it would be desirable for there to be a mechanism whereby such interpretations are brought to public attention.

66. At present under RIPA this would only occur in the event of a complaint in the IPT or a legal challenge by a service provider against a warrant or notice. The position under the draft Bill is similar. It contains, as far as I can discern, no mechanism to ensure that interpretations are proactively brought to public light.

67. That this is a real issue is illustrated by the Home Office's interpretation of 'external communications' under RIPA, revealed in a witness statement of Charles Farr in the *Liberty* case in the IPT.

68. The background was that under RIPA S.8(4) GCHQ can intercept in bulk if its purpose is to intercept external communications. So the meaning of 'external communications' is significant.

69. The Home Office interpretation was controversial. It also had implications for who (or what) could be regarded as a sender or intended recipient of a communication, a basic building block of RIPA. (See further paragraphs 6.52 and 12.25 of A Question of Trust and paragraphs 31 to 54 of my submission to the Anderson Review.)

70. The Home Office's interpretation, which underpinned the agencies' operations under RIPA S.8(4) warrants, would not have seen the light of day had the NGOs not brought the IPT legal challenge. That occurred because of the Snowden disclosures.

71. Another example is provided by DRIPA. It was said that the DRIPA amendments to RIPA's territoriality provisions and to the definition of telecommunications services did no more than reflect what the legislation had always meant. Those assertions were untestable, since the public had no way of knowing how the government might previously have interpreted the provisions either in the minds of its officials or in its previous dealings with communications service providers.

72. A similar issue could arise with the possible effect on end to end encryption of the draft Bill. This is a controversial topic, in its own right and also because Clause 189(4)(c) of the draft Bill can be compared with paragraph 10 of the Schedule to the 2002 Maintenance of Interception Capability Order (although the clause would apply in a much wider context, to a broader range of service providers and is drafted as an instance of a broader power). On the face of it at least some types of end to end encryption are applied not by a service provider but by the user. However the public is in no position to know whether the Home Office has previously adopted some other interpretation, nor (if the provision were to remain in its current form) what interpretations it might adopt in the future.

73. The draft Bill provides an opportunity to ensure that the proposed new oversight body proactively seeks out and brings to public attention material legal interpretations on the basis of which powers are exercised or asserted. Service providers might usefully also be able to bring a legal interpretation asserted against them to the attention of the oversight body, which would have to bring it to public attention. A procedure of this kind may be all the more necessary in the light of the new disclosure restrictions included in the draft Bill.

74. Such mechanisms would enable material legal interpretations to be publicly debated and if appropriate challenged. None of this would require to be made public any legal advice that the government had received, nor any factual matters that should properly remain secret, but only the substance of the legal interpretations themselves.

75. This would contribute to openness and transparency. By providing not only oversight but insight it would help to satisfy the requirement that the law should be foreseeable and accessible.

LEGAL PROFESSIONAL PRIVILEGE

Q.10 WHAT IS THE LEGAL STATUS OF THE CODES OF PRACTICE UNDER RIPA? WHAT DO YOU EXPECT TO BE CONTAINED IN THE CODES OF PRACTICE ISSUED UNDER THIS BILL?

76. Although the topic of Codes of Practice is raised here under LPP, it raises more general issues about the relationship between the text of the draft Bill and Codes of Practice.

Legal status of Codes of Practice

77. The legal status of Codes of Practice under the draft Bill is differently expressed from that under RIPA. S.72(4) RIPA assigns a general interpretative function ("relevant to any question arising in the proceedings… taken into account") to Codes of Practice issued under S.71. This function is omitted from the draft Bill. Under the draft Bill

(Schedule 6 para 7) Codes of Practice are generally admissible in evidence, but the only context specifically mentioned is a failure by a person to have regard to a Code.

Contents of Codes of Practice

78. The contents and quality of existing Codes of Practice vary. In some respects they can resemble an expanded set of Explanatory Notes. They are most useful and appropriate when fleshing out practice, processes and methodologies. The Interception and Communications Data Acquisition Codes of Practice are good examples.

79. Codes can also usefully provide uncontroversial illustrative examples. The Communications Data Acquisition Code has 5-6 helpful pages of explanation and examples of traffic data, subscriber data and service usage data.

80. It should not, however, be the role of Codes to fill substantive gaps in the parent statute, nor to interpret opaque or poorly drafted provisions of the parent statute. If the parent statute is clear and appropriately drafted, then the Code of Practice can follow suit. If the parent statute is muddled, opaque or obscure, the Code of Practice may compound the confusion and create controversy in its attempts to explain the statute.

81. It may be suggested that Codes of Practice can be used as a means of providing flexibility and thereby future-proofing powers granted by legislation against technological change. My own view is that this is not an appropriate use of Codes of Practice, for the reasons set out in the section on Future-Proofing. Even where Codes of Practice are required to be placed before Parliament they may not receive the scrutiny appropriate to what might, in effect, be updating legislation.

DATA RETENTION

Q.14 IS THE RETENTION OF DATA FOR 12 MONTHS A PROPORTIONATE BALANCE BETWEEN THE NEEDS OF THE SECURITY SERVICES AND LAW ENFORCEMENT AND THE RIGHTS OF THE INDIVIDUAL?

Preliminary: 'retention'

82. Current legislation (DRIPA, as amended by CTSA 2015) is limited to retention properly so called: retention of data already generated or processed in the United Kingdom by public telecommunications operators in the process of supplying the telecommunications services concerned.

83. Although the powers under Clause 71 are labelled 'retention' they go much further. Clause 71(8)(b) includes generation of data for retention and obtaining of data for retention. On their face these are both significant extensions over the existing data retention legislation.

84. It seems that Clause 71(8)(b) (a provision that approaches RIPA standards of impenetrability) could even be read as providing the power to require service providers to conduct 3rd party data retention. Presumably that is not the intention,

since 3rd party data retention is an aspect of the draft Communications Data Bill that the government has disavowed.

85. Clause 71(8)(b) may perhaps also provide the power to require a service provider to require a third party, such its customer, to create data in order to provide it to the service provider.

86. If that is right, then could a data retention notice be used to require (say) the operator of a public Wi-Fi facility or an internet café to obtain and retain names and address details of its users? Some may think that would be a good thing. Others would deplore it. Either way, it does not seem right that a decision to impose an obligation of such significance could be made by way of a secret instruction of the Home Secretary based on an obscurely worded statutory power.

87. As to generation of data, the evidence of service providers to the Committee has suggested that ICRs do not exist as such on their systems. If they have to be created the power to require data to be generated assumes considerable significance.

Preliminary: essence of the right?

88. Question 14 is couched in terms of proportionality. However compulsory generation, obtaining and retention of communications data (in particular ICRs) may touch on a prior issue, namely whether the retention requirement respects the 'essence of the right'.

89. Respect for the 'essence of the right' is explicitly recognised in Article 52 of the EU Charter.

90. The CJEU in *Digital Rights Ireland* considered whether the retention required by the EU Data Retention Directive violated the essence of the privacy right under Article 7 of the Charter. It held not:

> "… even though the retention of data required by Directive 2006/24 constitutes a particularly serious interference with [Article 7] rights, it is not such as to adversely affect the essence of those rights given that … the directive does not permit the acquisition of knowledge of the content of the electronic communications as such."

ICRs and itemised phone bills

91. Destination data ICRs differ from the communications data considered in *DRI*, in that arguably they may possess some of the qualities of content.

92. As well as affecting privacy rights mandatory retention of destination data ICRs would engage the right of freedom of expression.

93. This may seem a bold claim in the face of the oft-repeated assertion that ICRs are nothing more than the online equivalent of an itemised phone bill. The Home Secretary, introducing the draft Bill, said:

> "So, if someone has visited a social media website, an Internet Connection Record will only show that they accessed that site, not the particular pages they looked at, who they communicated with, or what they said. It is simply the modern equivalent of an itemised phone bill."

94. If a comparison can be drawn with an itemised phone bill, this would be an itemised phone bill like none ever seen[1295]. We can illustrate this by considering the questions that could be answered by scrutinising an actual itemised phone bill compared with one containing the destination information that would be logged in an ICR.

Who has she spoken to?

95. This is the focus of the traditional itemised phone bill.

96. The itemised phone bill shows called telephone numbers. In pre-online, pre-mobile days it would have been a fair assumption that whoever was using the telephone was speaking to somebody at the called number, so that a conversation took place[1296]. That might be somebody at a household telephone or at a public telephone box. The number might be a private office switchboard[1297], at which point the information on the itemised phone bill terminated. It gave no information about which extension the call was routed to behind the private switchboard, or who took the call at that extension[1298]. (The former changed to an extent with the advent of DDI numbers.)

97. A subscriber lookup would provide information about the householder or organisation to whom the called number was allocated.

98. Itemised phone bills have always, with a few exceptions (e.g. dial-up data calls, recorded message services) essentially given information (including when the call was made and its duration) about conversations between human beings.

What has she been doing?

99. Our notional ICR itemised phone bill now starts to part company from an actual itemised phone bill. It is possible to infer a partial picture of someone's activities by studying a record of whom she has talked to on the telephone. ICR logs differ in both degree and kind.

100. ICRs differ in degree in that we now speak on mobile phones and send text, e-mail, SMS and all the other varieties of messages to people in vastly greater volumes than we ever did in the days of landline telephone conversations. This itself provides a

---

1295 Nor should we forget that when itemised phone bills first appeared they excited alarm as to how revealing of people's personal lives they could be.

1296 Of course other possibilities existed, such as sending a coded signal by a pre-arranged sequence of calls and hang-ups. Nevertheless there was still a communication between two people.

1297 The public telephone number of an office switchboard is somewhat equivalent in the internet world to an ISP allocating one public IPv4 address to the household or office router rather than allocating multiple public IPv4 addresses to individual devices in a household. An ISP allocating a public IPv4 address to one individual device in the household or office is a bit like what used to be called a 'direct outside line'.

1298 It is somewhat ironic that the example on page 9 of the ICR Operational case gives 4 digit extension numbers as an example of something equivalent to a port number. A private extension number would never appear on an itemised phone bill. An 'extension' would have appeared on a bill only if the caller dialled a direct line or a DDI number.

vastly richer and more detailed map of our activities than ever was possible with an itemised phone bill.

101. ICRs differ in kind from an itemised phone bill in that they are not limited to our conversations (whether voice, e-mail or messages) with other people. An ICR is an itemised phone bill that would log not just whom we conversed with when, but our online journeys: our 'visits' to the bank, the bookshop, the butcher, the baker, the travel agent, the doctor, the clinic, the hospital, the therapist, the support group, the hotel, the club, the concert hall, the public lecture, the political meeting, the trade union office, the ticket agency and so on without limit.

102. It would go further, logging not just our consciously initiated activities but also those initiated by our smartphones and connected tablets while they are in our pockets, beside our beds at night and so on.

103. In this respect ICRs bear little resemblance to an itemised phone bill. If anything they are more akin to universal CCTV surveillance when we step out beyond our front door and venture into public spaces. However that analogy is itself debatable.

What has she been reading?

104. ICRs would create logs of every website (or equivalent) that we accessed. On my understanding of the draft Bill that would include blogs and newspaper sites[1299].

105. In this regard ICRs are far removed from both itemised phone bills and CCTV in public places. They do not resemble any kind of log that it has been thought appropriate to compel in the offline world. It is as if, on our notional itemised phone bill, we were to find a state-mandated list of the titles of the books, newspapers and magazines that we had read in the last 12 months.

106. We never used to read books over the telephone. Now we read blogs remotely. It is a mere accident of technology that by doing that, instead of reading a physical book in an armchair at home, we engage in what the draft Bill (and RIPA before it) classifies as a 'communication'.

107. DRIPA was limited to something that people would generally regard as an online communication: internet e-mail, SMS messages and the like. Reading something remotely, however, is not a communication in the sense of a group of conspirators discussing criminal plots between themselves. It is a highly personal activity of one individual alone.

108. Someone who accessed my own blog could[1300] trigger the creation of an ICR showing that they had accessed 'cyberleagle.blogspot.co.uk' (the URL up to the first slash), or

---

[1299] The assumption in the draft Bill appears to be that all websites would be covered by 'telecommunications service' in Clause 47(6)(a) (see e.g. the Guide para 44). A scheme that required service providers subject to a retention notice to determine whether individual websites were or were not providing a 'telecommunications service' would presumably be unworkable. If a site were subject to retention under the (differently worded) Clause 71 but fell outside Clause 47(6)(a), then it would not be subject to the access restrictions of Clause 47(4).

[1300] If only the destination IP address were logged and not the blog's web address that might show only that the Blogger platform was accessed.

maybe 'www.cyberleagle.com' if they used that address. The ICR might record the name of the blog: 'Cyberleagle'. It would record the date and time of the access[1301]. It would presumably have to be linked at least to source data identifying (to the extent possible) the device that accessed the blog.

109. Mandating that logs of online reading habits be kept is analogous to being made, in the offline world, to keep a list of the books, newspapers and magazines that we have read in the last year.

Privacy, freedom of expression and logging reading habits

110. Reading is in the nature of a home activity. We are far more cautious about the intrusion of general powers into the home. We treat with greater respect for privacy activity takes place there than activity that takes place in public or semi-public places[1302]. When considering online activities we should always consider whether the activity in question is an extension of the home or an excursion into a public or semi-public place.

111. State-mandated lists of reading habits also strike at the heart of freedom of expression. Our freedom to choose what to read is jealously protected for good reason. Reading fuels our quest for knowledge. It is emancipatory[1303]. Merely making an officially mandated list of what we choose to read chills freedom of expression. If the ordinary citizen is put in the position of worrying about whether reading a controversial website might excite official suspicion or trip a red flag on some state computer system, that alone is sufficient to chill freedom of expression whatever the safeguards and restrictions on access.

112. A proposed law requiring us to make and keep a list of physical books, newspapers and magazines that we had read in the last 12 months could expect to be greeted with public outrage. This aspect of ICRs is an exact parallel.

113. Reading is also a large part of the 'online visiting' aspect of ICRs. The two are inextricably entangled.

114. Even if 'reading' websites could somehow be conceptually separated from 'visiting' websites, it is difficult to envisage any practicable way in which ICR retention could be implemented for only some types of website. Either way, the whole proposal would stand or fall with the 'reading' element.

BULK INTERCEPTION WARRANTS

1301 The ICRs Fact Sheet says: "[An ICR] will involve retention of a destination IP address but can also include a service name (e.g. Facebook or Google) or a web address (e.g. www.facebook.com or www.google.com) along with a time/date."

1302 Red Lines and No Go Zones: the coming surveillance debate http://cyberleagle.blogspot.co.uk/2015/07/red-lines-and-no-go-zones-coming.html.

1303 "Theresa May's Threat to the Privacy of Reading" John Naughton www.theguardian.com/commentisfree/2015/nov/08/theresa-may-proposals-privacy-reading-draft-investigatory-powers-bill

Q.16 SHOULD THE PRESENT POWERS RELATING TO BULK INTERCEPTION WARRANTS BE REPLICATED IN THE DRAFT BILL OR SHOULD WARRANTS BE MORE NARROWLY FOCUSED AS TO THEIR PURPOSE AND PERMITTED SEARCH CRITERIA?

115. The existing RIPA bulk interception warrant provisions have two distinct aspects: content and related communications data.

116. As to **content**, see my analysis of RIPA in 'The tangled net of GCHQ's fishing warrant' (http://cyberleagle.blogspot.co.uk/2015/01/the-tangled-net-of-gchqs-fishing-warrant.html) The equivalent provisions in the draft Bill are generally similar, although the following are noteworthy in connection with points mentioned in my analysis:

- External communications are now replaced by overseas-related communications. While this governs the overall purpose of the interception, as with RIPA once communications (whether overseas-related or collaterally intercepted non-overseas-related) have been intercepted they form a common pool. No further distinction is made and there is no obligation (at least no express obligation) to identify and discard non-overseas-related communications.

- The draft Bill puts beyond any doubt (119(4)(a)) that for the purposes of selection for examination the relevant time for considering whether a person is within the British Islands is the time of the selection, not the time of the communication.

- The targeted examination warrant replaces the S16(3) modification.

- It is no clearer whether there is a dividing line between selection and examination, or whether examination can involve a continuing element of selection.

- The provisions regarding knowledge of a person's location are similar, other than 119(3)(b) which removes the RIPA requirement that the belief that the selection prohibition would not be breached must be held on reasonable grounds.

- The S.8(4) certificate is replaced by 'specified operational purposes'. Although the operational purposes cannot simply recite the statutory purposes (national security, prevention or detection of serious crime, national security-related UK economic well-being) they can still be general purposes (111(4)). (Curiously, the Home Office Guide refers throughout to 'specific' operational purposes.)

117. As to **related communications data**, appreciating the potential scope of this power remains (as with RIPA) a matter of chaining together collateral powers in a way that is not immediately obvious on the face of the statute.

118. This is one area in which it is no exaggeration to say that GCHQ collects *all* data (ISC Report March 2015, para 134):

> iii) **Related CD (RCD) from interception:** GCHQ's principal source of CD is as a by-product of their interception activities, i.e. when GCHQ intercept a bearer, they extract all CD from that bearer. This is known as 'Related CD'. GCHQ extract all the RCD from all the bearers they access through their bulk interception capabilities (as covered in the previous chapter).

119. A case could be made that a power of such potential reach (and the applicable restrictions on it) should be made clearer on the face of the statute. This power does not appear separately in the table of Powers at a Glance annexed to the Home Office Guide (I have prepared and annex a fuller version of the table).

120. Comparing the draft Bill with RIPA:

- Related communications data is made subject to 'specified operational purposes' (see above) rather than only being subject to the overall statutory purposes.

- The scope of the power is increased by the ability to treat communications data extracted from content as related communication data (106(8)).[1304]

- The structure of the RCD power is replicated (i.e. no British Islands selection restrictions) for bulk equipment interference 'equipment data' (136(4)). Similarly there is provision for equipment data extracted from content (147(8)). As with RCD the bulk communications data acquisition power (Part 6 Chapter 2) is not subject to any British Islands selection restrictions.

121. Given the far reaching potential scope of these powers it is pertinent to ask: How has the RCD power been used to date? How could the powers be used under the draft Bill?

122. There are three sources of information about how the RCD power has been used to date.

123. The first is the Interception Commissioner's Report for 2014, published in March 2015. The Commissioner reported the results of its review of the use by agencies of (amongst other things) Related Communications Data. He said:

> "6.63 Although my office's investigation demonstrated that indiscriminate retention for long periods of unselected intercepted material (content) does not occur and the interception agencies delete intercepted material (if it is retained at all) after short periods, and in accordance with section 15(3) of RIPA 2000, I reported that *related communications data* are in some instances retained for a variety of longer periods and that I had yet to satisfy myself fully that some of the retention periods were justified.
>
> 6.64 This investigation led my office to make 22 specific recommendations in 2013 and 11 specific recommendations in 2014 for the interception agencies to review or shorten their retention periods and/or destroy intercepted material and/or related communications data where there was no persuasive justification provided for its

[1304] This assumes that data within 106(8) ceases to be content once extracted.

ongoing retention. A number of the 2014 recommendations were to ensure that the interception agencies remained focused on the issue, to boost their efforts to review their retention periods or destroy certain material, and to create a corporate culture of reviewing regularly and destroying material and data when it is no longer necessary and proportionate to retain it.

6.65 I can report that all of the recommendations were accepted by the interception agencies. The large majority have already been fully implemented. *This has caused a significant amount of intercepted material and related communications data to be destroyed, and in some instances entire systems have been decommissioned.* In other cases the maximum retention periods have been halved. Those agencies which have not yet managed to implement the recommendations in full are waiting on significant technical changes to be made to IT systems. I have made clear that future retention and destruction policies should not be dependent on broad assumptions about the value of the material or data. Reviews should be conducted regularly, informed by profiling exercises to ensure that the retention and destruction policies are not arbitrary. I welcome the progress made and my office will continue to monitor this area of the process." (emphasis added)

124. The second source is the December 2014 judgment of the Investigatory Powers Tribunal in the *Liberty* case. The complainants argued that RIPA's relatively loose restrictions on use of intercepted communications data could mean that, in the words of the Tribunal's judgment:

"a database can be built up of communications data (including communications data not excluded by s.16(2), as discussed above) so as to justify a continuing databank, continuously renewed by reference to the continued necessity for it for one of the s.5(3) purposes, not necessarily being the statutory purpose for which the communications data was originally intercepted."

125. The Tribunal went on:

"139. We are satisfied as a result of what we saw and heard at the closed hearings, and the further Disclosure set out above, that this is not the case and that there are adequate arrangements, in respect of duration of retention and destruction, to control and regulate the retention of such material. Such retention, storage and destruction policies and procedures are also regularly supervised by the Commissioner, as he makes clear in his Report."

126. The government Disclosure referred to included the following passage:

"As regards related communications data in particular, Sir Anthony May made a recommendation to those of the Intelligence Services that receive unanalysed intercepted material and related communications data from interception under a s8(4) warrant, and the interim Commissioner (Sir Paul Kennedy) has recently expressed himself to be content with the implementation of that recommendation."

127. Exactly what this may mean in terms of the retention and use of RCD is not clear. However the value placed on it by the agencies is not in doubt. The ISC in its March 2015 Report said:

> "80. We were surprised to discover that the primary value to GCHQ of bulk interception was not in reading the actual content of communications, but in the information associated with those communications. This included both Communications Data (CD) as described in RIPA (which is limited to the basic 'who, when and where' and is described in greater detail in Chapter 6), and other information derived from the content (which we refer to as Content-Derived Information, or CDI),74 including the characteristics of the communication75 ***. While CDI is not what might be most obviously understood to be content, under RIPA it must be treated as content, not CD. Examination of CDI therefore requires the same Ministerial authority as examination of content."

128. The government argued before the IPT that the absence of examination restrictions on RCD was justified by its use in order to determine whether someone was for the time being within the British Isles. This was necessary in order for the safeguard in Section 16(2)(a) to work properly:

> "In other words, an important reason why the Intelligence Services need access to related communications data under the s.8(4) Regime is precisely so as to ensure that the s. 16 safeguard works properly and, insofar as possible, factors are not used at the selection that are - albeit not to the knowledge of the Intelligence Services - "referable to an individual who is ... for the time being in the British Islands"." [112]

129. The IPT accepted that the different treatment of communications data

> "is justified and proportionate by virtue of the use of that communications data for the purpose of identifying the individuals whose intercepted material is to be protected by reference to s.16(2)(a)."[114]

130. The IPT rejected the NGOs' argument that use of communications data for this purpose could be addressed by an exception in the legislation, saying that it was an "impossibly complicated or convoluted course".

131. The third source, more controversially, is the batch of Snowden documents published by The Intercept in September 2015 (https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities/). These refer to various GCHQ events databases, including one called KARMA POLICE:

> "KARMA POLICE aims to correlate every user visible to passive SIGINT with every website they visit, hence providing either (a) a web browsing profile for every visible user on the internet, or (b) a user profile for every visible website on the internet."

132. 'Visible to passive SIGINT' appears to be a reference to bulk interception. There is mention of a prototype 17.8 billion row KARMA POLICE database representing 3 months' data. As an events database (thus apparently containing no content) it can be assumed that KARMA POLICE would fall under the looser RCD examination regime.

133. Whether or not KARMA POLICE (or something like it) may exist today, a hypothetical KARMA POLICE is an interesting touchstone against which to test the draft Bill.

134. No doubt there will be differing views about whether it should be possible to use bulk warrants to build a hypothetical KARMA POLICE database, and if so whether the restrictions on the ability to search it should be tighter than the statutory purposes, specified operational purposes and necessity and proportionality.

135. But the prior question is would such a database be possible under the draft Bill? If so, given the new proposed ability to extract related communications data from content (corresponding to CDI as described in the ISC Report?), would a hypothetical "KARMA POLICE PLUS" be possible? Could such a database be fed from multiple sources (such as the communications data and equipment data product of bulk equipment interference and bulk communications data acquisition warrants)?

136. If nothing like this is intended to be possible, then the powers could and should be drawn more narrowly to reflect what is intended and to enable the debate to be framed accordingly. One question might be whether it is as impracticable as the IPT suggested to limit the use of RCD to identifying individuals who would qualify for the 'known to be within the British Islands' protection.

137. If the ability to build a hypothetical KARMA POLICE is intended, then the question arises whether it is appropriate for a universal database of internet browsing profiles (both domestic and foreign) to be capable of being built as a by-product of powers whose overall purpose is the interception of communications with an overseas element.

Nothing to hide, nothing to fear

138. RCD powers are a pertinent context in which to reflect on 'nothing to hide, nothing to fear'. It is a powerful slogan that strikes a chord with many, in the UK perhaps the majority of, people who are certain that we have nothing to fear from a benign state that is only trying to do its job to protect us: 'GCHQ is welcome to read my e-mails any time they like. They won't find anything to interest them."

139. Many thousands of words, books indeed, have been devoted to counter-arguments. An immediate response, such as in a recent publication by the Open Rights Group (www.openrightsgroup.org/blog/2015/responding-to-nothing-to-hide-nothing-to-fear), is that even the most law abiding people have many legitimate reasons to keep things private. Whilst certainly true, that may cut little ice when you see the state as your trusty guardian angel: 'Law enforcement has an important job to do. Only criminals could object. That's not me.'

140. If an intelligence agency were to judge you only by what you said in your own texts and e-mails perhaps you could know that you have nothing to hide. (Although are you really sure that everything you have written was not open to misinterpretation? That you could always explain what someone else sent you? A modern day Cardinal Richelieu would have considerably more than six lines to work with.)

141. But a willingness to hand over your private life to a stranger misses the point that 21st century state surveillance is not just about our own lives. In a world of mass data capture and computerised analysis aimed at discovering new suspects it is as much about the company we keep, the places we visit and the patterns we weave online: our associations.

142. We may trust our online associates. But we cannot see inside their minds. We know little of their present, less of their past and nothing of their future. We know less than nothing about our associates' associates.

143. In his report for 2013 Sir Anthony May, the then Interception of Communications Commissioner, sought to reassure the public that it has nothing to fear from GCHQ's mass interception activities:

> "I am, however, personally quite clear that any member of the public who does not associate with potential terrorists or serious criminals or individuals who are potentially involved in actions which could raise national security issues for the UK can be assured that none of the interception agencies which I inspect has the slightest interest in examining their emails, their phone or postal communications or their use of the internet, and they do not do so to any extent which could reasonably be regarded as significant."

144. But how can any member of the public be certain that there is no 'potential' malefactor among their online associates? How can anyone know that they have nothing to hide, even from agencies acting with complete good faith and conscientiousness?

Amended Home Office 'Investigatory Powers at a Glance'					
	Conduct authorised	**Statutory bodies/purposes**	**Authorisation – Acquisition**	**Authorisation - Access**	**Oversight**
Targeted (13(1)) and Thematic (13(2)) Interception (14(1))	Obtaining the content of a communication in the course of its transmission (12(2)(a)) Obtaining related communications data (RCD) from communications described in the warrant (12(2)(b))	5 law enforcement agencies, MI5, GCHQ, SIS and the Ministry of Defence (15(1)) Purposes: National Security, Serious Crime and Economic Well-Being of the UK (14(3))	Secretary of State authorisation, subject to approval by a Judicial Commissioner before non-urgent warrants come into force (14(1)(d))	N/A	Investigatory Powers Commission (IPC) replaces the Interception of Communications Commissioner Office (IOCCO), the Office of Surveillance Commissioners (OSC) and the Intelligence Services Commissioner (IsCom). The judge-led IPC will have an extensive remit to oversee the use of all investigatory powers and will scrutinise those provided with these powers though
Communications Data (CD) (46)	Obtain CD, usually via Communications Service Providers (CSPs) (46(2)) ('any person')	Public authorities provided with the ability to acquire CD and statutory purposes (46(7)) will be listed in the Bill.	Must be authorised by a designated person (who must be independent from the investigation) following consultation with a single point of contact (SPOC) (60). [Only the SPOC can approach CSPs to request CD] (??)	N/A For ICRs, restricted to 3 specified purposes; local authorities excluded (47(4) and (5))	
Targeted (81(1)(a)) and	Obtaining private data	MI5, GCHQ, SIS, (84) law enforcement (89) and the	Secretary of State authorises warrants for MOD and security	N/A	

Thematic (83(b)) Equipment Interference (EI) (lawful interception authority for stored communications only (5(1)(a)(ii), 81(6))	covertly from computers and other equipment (communications, private information, equipment data – comms data, system data, extracted CD) (81, 82)	Ministry of Defence (87) Purposes: National Security, Serious Crime and Economic Well-Being. Law enforcement may only seek warrants for serious crime (89).	and intelligence agencies. (84, 87) Chief Constable authorises law enforcement use. (89) All non-urgent warrants subject to Judicial Commissioner check before coming into force (84(1)(d), 87(1)(d), 89(1)(d)).		inspections, investigations, audits and authorisations of warrants and internal practices. Statutory Codes of Practice will outline further details.
Bulk Powers (Bulk EI: lawful interception authority for stored communications only (5(1)(a)(iv), 135(5))	Bulk interception (106) (obtaining content and related communications data (RCD) (106(4)(b), 106(5)(a)(ii))) Bulk Equipment interference (135)(1)(b) Obtaining private data	MI5, GCHQ, SIS (107(1), 137(1)), 122(1). Purposes: overseas-related (Bulk interception (106(2)(a)) and Equipment Interference (135(1)(c))); Bulk Acquisition not so restricted other than Economic Well-Being (122(3)) Warrants must be necessary in the interests of national security; may also be authorised for Serious	Secretary of State authorises warrants, subject to approval by a Judicial Commissioner Interception and equipment interference warrants (but not data acquisition warrants) must be targeted at persons outside of the UK. (see previous column)	Examination of any material must be necessary for a specified Operational Purpose (which can be general (111(4)), 140(5)), 125(4)), authorised by a Secretary of State and approved by a Judicial Commissioner. Examination of content relating to persons in the UK requires a separate targeted warrant. That requirement does **not** apply to:	

	covertly from computers and other equipment (communications, private information, *equipment data – comms data, system data, extracted CD*) (135, 136) Bulk acquisition of Communications data (122)	Crime and Economic Well-Being (107(1)/(2), 137(1)/(2), 122(1)/2))		Bulk interception: related communications data (because omitted from 119(1)(c)) Bulk equipment interference: equipment data or non-content information connected with the equipment 147(1)(c), 147(8)) Bulk acquisition of communications data, by its non-content nature	
Bulk Personal Datasets (BPD) (150)	Additional safeguards for the acquisition and use of BPD	MI5, GCHQ, SIS Purposes: National Security, Serious Crime and Economic well-being	Authorisation to acquire particular classes of BPD issued by Secretary of State and subject to approval by a Judicial Commissioner	Examination of any material must be necessary for a specified Operational Purpose (153) (no provision saying may be general), authorised by a Secretary of State and approved by a Judicial Commissioner.	
National Security Notices?					
Technical Capability Notices?					

Graham Smith—supplementary written evidence (IPB0126)

22 December 2015

Graham Smith—further supplementary evidence (IPB0157)

1. Since I submitted my written evidence on 22 December 2015 the Home Office written evidence has been published. It contains, in Annexes A and B, considerably more detail than has previously been made publicly available about the datatypes that the Home Office considers would be content or communications data and those that it considers would constitute Internet Connection Records.

2. The new information bears on some of my previous evidence, as to which I provide these further comments.

ICRs and third party data retention

3. In my previous written evidence I said at paragraph 84:

   "It seems that Clause 71(8)(b) (a provision that approaches RIPA standards of impenetrability) could even be read as providing the power to require service providers to conduct 3rd party data retention. Presumably that is not the intention, since 3rd party data retention is an aspect of the draft Communications Data Bill that the government has disavowed."

4. Three types of ICR destination data were mentioned in the Home Office ICR Fact Sheet: (1) web addresses (such as www.bbc.co.uk), (2) service names (such as Facebook or Google) and (3) destination IP addresses. The double asterisk footnoted items in the table at Annex A paragraph 20 of the Home Office written evidence acknowledge that web addresses and server (sic) names may be 3rd party data:

   > "** This may be third party data when seen by an internet access provider."

5. Thus the Home Office appears to confirm that retention (or generation or obtaining) of ICRs containing destination data other than IP addresses can in fact be a form of 3rd party data retention. That is consistent with and reinforces my concern that Clause 71 is broad enough to cover 3rd party data retention generally.

6. We then find the following statement in Annex B under "What is an Internet Connection Record?"

   > "The URI domain or service identifier may, depending on how a CSP configures its network, constitute 3rd party data. *Unless a CSP process that data themselves for business purposes it cannot be retained as part of an ICR.*" (emphasis added)

7. The first sentence provides further confirmation that the first and second types of ICR destination data are (or at least may be) 3rd party data. The second (italicised)

sentence appears to reflect the government's disavowal of 3rd party data retention (if that means mandated capture of 3rd party communications data that the ISP would not otherwise perform).

8. However the limitation to data processed by a CSP for its own business purposes does not exist in Clause 71. That limitation would require the introduction of something akin to the existing DRIPA limitation of 'generated or processed in the UK'. Not only was that limitation abandoned in Clause 71 but new powers to require not merely retention but the generation and obtaining of data were introduced (my previous evidence, paragraph 61).

9. My previously expressed concern that as it stands Clause 71 could be read as empowering 3rd party data retention is further reinforced. The clause appears to require significant revision to do no more than give effect to the Home Office's currently stated intention. That is quite apart from the questions of whether the Clause 71 power is any case far too broad, or should exist at all.

10. As cited in footnote 12 of my previous evidence the ICR Fact Sheet states that an ICR 'will' involve retention of a destination IP address but 'can' also include a service name or web address. That distinction may now assume more significance. I observe in passing that the ICR Operational Case provides no detail about the relative usefulness of destination IP addresses (which could represent anything from a website, or a collection of unrelated websites, to a home or office router to a network gateway) compared with service names or web addresses, for achieving the three stated Purposes.

Content versus communications data: "URLs up to the first slash"

11. In the table at Annex A para 20 of its written evidence the Home Office classifies as 'content' the following:

> "The url of a webpage in a browsing session (e.g. www.bbc.co.uk/news/story or news.bbc.co.uk or friend'sname.facebook.com)"

12. The first example reflects the existing understanding that a full URL is content. The second and third examples (subdomains) differ from the understanding recorded at page 137 footnote 32 of 'A Question of Trust':

> "The Home Office has indicated that such data could include but is not limited to: - <u>url addresses</u>: Under the current accepted distinction between content and CD, www.bbc.co.uk would be communications data while www.bbc.co.uk/sport would be content; and this is set out in the Acquisition Code. However there are arbitrary elements to that definition – for example sport.bbc.co.uk (no 'www.') takes you to the same place as www.bbc.co.uk/sport."

13. The change is presumably intended to address the noted element of arbitrariness. However I cannot see anything in the definitions of content, communications data or the provisions of Clause 71 as they currently stand that would draw the line at the point now suggested.

14. The Home Office position as stated in its written evidence would appear to mean that a blog address in the form cyberleagle.blogspot.co.uk (see paragraph 108 of my previous written evidence) could not be retained in full as part of an ICR, whereas one in the form www.cyberleagle.com would be. This does not affect the thrust of my evidence regarding reading activities on the internet.

11 January 2016

Winston Smith—written evidence (IPB0062)

1) As invited by the Joint Committee, I write concerning the draft Investigatory Powers Bill, also concerning the 'Operational case for the retention of Internet connection records' published with it.

2) With regard to "Overarching/thematic questions", a fundamental question which the Committee has not asked is whether this country belongs to its citizens, or whether the citizens belong to the state. It seems to me that the citizens are not the property of the state, and thus citizens and other residents should go about their *lawful* business free from any deliberate observation or recording by the state of their communications and free from intrusion by the state into their homes, offices or property, including freedom from interference by the state with their computing and communications devices.

3) A related fundamental question is whether the fact that most citizens have nothing to hide therefore entitles the state to keep a record anyway, supposedly without causing offence but in the vast majority of instances *simply to record what the innocent citizen is doing*. The right of the citizen to his or her private life means that the former does not justify the latter: instead, infringement of a citizen's privacy by the state must rest on the state having grounds for suspicion sufficient to convince a judge.

4) Supposing that citizens have the right to conduct their private lives and lawful private business without the state prying, another overarching question not mentioned by the Committee is what rights to redress and to compensation should exist for wrongful infringement of a citizen's privacy by the state - on the same lines as the citizen's right to redress and to compensation for wrongful arrest and for unlawful imprisonment, i.e. when a citizen's freedom of lawful movement is infringed unlawfully by the state.

5) A further fundamental question which the Committee has not asked is whether watching the innocent, by far the *vast* majority, in going about their *lawful* business can ever be a useful way to observe a *very* small minority going about their *very criminal* business. In my opinion, watching the innocent *en masse* by means of technology is no substitute for getting close to the seriously-criminal.

6) A related fundamental question not asked by the Committee is whether the nature of the security services in the field is an obstruction to their ability to get close to, for example, terrorists.

7) It has been said of the FBI and the CIA that more and more staff are devoted to office-based work, and fewer and fewer to field work, producing an ever-larger budgetary requirement but to the detriment on their ability to tackle serious criminals.

8) The government intends to recruit more staff for MI5 and GCHQ; I expect that the majority of these will be white and middle-class and will not be based in the field but instead in the office, nor will they speak Arabic, Urdu, Pashtu, nor any African language, especially not as a native tongue.

9) I expect that they will not be former terrorists, people-traffickers, arms dealers, or drug smugglers either, and I hope that they will not be paedophiles nor child-pornographers. While being of a different ilk may pose a problem for security staff in knowing how to get close to such criminals, mass surveillance of the innocent is not likely to assist.

10) Just as in the case of counter-espionage and the apprehension of spies, mass surveillance by white men in the office or in a computer centre such as GCHQ is not likely to compensate for inability to get close to the criminal.

11) With regard to whether the proposed measures to infringe citizens' privacy are proportionate, it is necessary first to see whether they are likely to be effective.

12) Rather than considering the proportionality of mass surveillance (without grounds for suspecting the whole populace of petty crime, let alone of serious crime), the Committee should consider instead the availability, under warrant from a judge, of the truly vast amount of private-sector information concerning the behaviour of almost anyone in modern times, as well as what might be had by interception of internet and telephone traffic under warrant.

13) The proposal to record the addresses of sites visited on the internet by members of the public is unlikely to inconvenience the seriously-criminal. The published 'Operational case' (the portable document format version of which one can search readily) contains no reference to virtual private networks, to the OpenVPN protocol, to proxy servers, to 'onion routers' such as TOR, nor to encryption. These, and other readily-available associated means, enable many people to use the internet already without their ISP knowing which sites they visit (and without others knowing where the user is located). The document makes no mention either of access from internet cafés and from libraries, nor by using public Wi-Fi networks.

14) It is easy also to communicate without visiting any web sites, but the 'Operational case' does not mention Skype used over virtual private networks, personal-key encrypted secure exchange of messages, nor communicating anonymously by use of public telephones and of buy-and-discard simple mobile telephones, let alone by post and face-to-face.

15) The case studies appended to the 'Operational case' are not said to bring about the arrest of terrorists nor of arms dealers (neither term being found in the whole document), which is realistic, unfortunately, given the means described therein.

16) It seems to me that the 'Operational case' was written either by people woefully ignorant of modern technology, or with the intention of misleading members of the legislature into continuing the recording of the readily-attributable (only) telephone use, and allowing the recording of the readily-attributable (only) internet use, of the vast majority of British residents for no good reason - the ones who are easy to watch because they are in settled residence and settled occupation, and who communicate naïvely because they have nothing to hide. These are the people whose use of their own telephones has been recorded, I gather, for the last ten years.

17) That, and the proposal to record also which web sites the innocent vast majority visit, seem to me an insulting infringement of the privacy of tens of millions of decent people to little or no effect, thereby also a great waste of public money.

18) I do hope that MPs will not allow the police, MI5 and GCHQ more power and more budget in order to intrude further, vainly, on the privacy of the innocent.

19) MPs should oblige the police and MI5 to explain instead how they will become close, personally, to terrorists, people- arms- and drug-traffickers, child-pornographers and

paedophiles. Such villains will not be uncovered by asking their ISP which web sites they visit, nor by asking their network providers which numbers they call from home or from a rented mobile device.

20 December 2015

Dr. Christopher Soghoian—written evidence (IPB0167)

Dr. Christopher Soghoian[1305]

21 December, 2015

I. Introduction

The Investigatory Powers Bill would explicitly permit the government to hack into computers, through the use of *targeted equipment interference warrants*.[1306] These warrants would not only permit the hacking of individual targets, but bulk hacking operations in which multiple devices, used or owned by multiple people, are hacked pursuant to a single order.[1307]

Since at least 2001, law enforcement agencies in the United States have used hacking and sophisticated surveillance software (commonly referred to by technical experts as malware) as part of criminal and national security investigations.[1308] As with many surveillance technologies used by the U.S. government, law enforcement agencies have intentionally kept the public in the dark regarding their use of this invasive technology.

In spite of the widespread secrecy regarding law enforcement hacking, enough information has come to light that I am able to describe a few specific public policy issues associated with, and in some cases, inherent in this use of this surveillance technology. If you do grant hacking powers to your law enforcement agencies, hopefully you will learn from our mistakes and include specific safeguards to protect the British public from the harms I describe in this document.

II. The use of deception and impersonation to deliver malware

Often, the most difficult part of a law enforcement hacking operation is the task of getting their surveillance software onto the computer of the target. If law enforcement agencies control a website that the target regularly visits or have physical access to the target's computer, malware delivery is relatively straightforward. Otherwise, they often have to try and trick the target into downloading a malicious email attachment or clicking on a malicious link in an email.

[1305] I submit these comments in my personal capacity. They do not necessarily reflect the views of my employer, the American Civil Liberties Union.

[1306] UK law enforcement agencies already hack, although, this was not known to the public or acknowledged by the government until this month. *See* Joseph Cox, UK's National Crime Agency Revealed to Have Hacking Powers, Motherboard, 5 Nov 2015, http://motherboard.vice.com/read/uks-national-crime-agency-revealed-to-have-hacking-powers.

[1307] *See* Draft Investigatory Powers Bill, Nov. 2015, Part 5, Equipment Interference, Section 83, Subject-matter of warrants, page 110 of https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf ("A targeted equipment interference warrant may relate to…(c) equipment belonging to, used by or in the possession of more than one person or organisation, where the interference is for the purpose of the same investigation or operation...(e) equipment in more than one location, where the interference is for the purpose of the same investigation or operation.")

[1308] *See* FBI Sheds Light on 'Magic Lantern' PC Virus, Reuters, 13 Dec. 2001, http://usatoday30.usatoday.com/life/cyber/tech/2001/12/13/magic-lantern.htm

Just as most drug dealers are unlikely to sell drugs to a police officer dressed in uniform, online criminals are unlikely to download an attachment or click on a link in an email if the sender is the Federal Bureau of Investigations or the National Crime Agency. As such, just as the police go undercover to conduct drug busts, law enforcement agencies also resort to deception and impersonation in order to deliver malware.

Impersonation and deception certainly make it easier for law enforcement agencies to successfully infect the computers of targets with malware. There are, however, significant public policy concerns associated with the use of impersonation by the government, particularly if and when the police impersonate doctors, lawyers, journalists, and the clergy, who can only perform their vital roles in our society if they are trusted by the public.

One year ago, while researching the Federal Bureau of Investigation's use of malware, I discovered that the agency had, in 2007, impersonated the Associated Press in an effort to trick a teenager into clicking on a malicious link in an email message.[1309] Although FBI agents had first sought and obtained a search warrant, the warrant application did not reveal to the court the means they intended to employ to deliver their malware, nor did they reveal that they planned to impersonate a journalist.[1310] Thus, the magistrate judge responsible for overseeing law enforcement's use of invasive surveillance techniques was only able to evaluate the invasion of privacy by the government—which was relatively modest, as the software merely collected basic information from the computer of the target. The court was unable to oversee the far more problematic aspect of this operation—the impersonation by the government of a trusted news organization. Indeed, it is quite possible that had the FBI agents told the court what they planned to do, the magistrate might have refused to approve the warrant.

Although news articles at the time had revealed the FBI's use of malware, the public remained in the dark regarding the agency's impersonation of a journalist until I revealed it in 2014.[1311] Once the FBI's use of this tactic was revealed, it was widely condemned by news organizations.[1312] In contrast, FBI Director James Comey defended his agency's impersonation of the Associated Press, calling it "proper and appropriate." Comey later told journalists that he was unwilling to forswear the use of similar tactics in the future, stating that "I'm not willing to say never. Just as I wouldn't say that we would never pose as an educator or a doctor."[1313]

[1309] *See* James B. Comey, To Catch a Crook: The F.B.I.'s Use of Deception, Letter to the Editor, New York Times, 6 Nov. 2014, www.nytimes.com/2014/11/07/opinion/to-catch-a-crook-the-fbis-use-of-deception.html ("[T]he online undercover officer portrayed himself as an employee of The Associated Press, and asked if the suspect would be willing to review a draft article about the threats and attacks, to be sure that the anonymous suspect was portrayed fairly. The suspect agreed and clicked on a link relating to the draft 'story,' which then deployed court-authorized tools to find him, and the case was solved.")

[1310] *See* Affidavit of Norman B Sanders Jr., Special Agent, Federal Bureau of Investigations, 12 June 2007, http://www.wired.com/images_blogs/threatlevel/files/timberline_affidavit.pdf.

[1311] *See* Christopher Soghoian (@csoghoian), Tweet, 27 Oct. 2014, 19:18 UTC, ("In 2007, FBI sent malware via a link intended to look like a Seattle Times/AP story. https://twitter.com/csoghoian/status/526815317390266368 at pages 61-62.")

[1312] *See* Chris Grygiel, FBI says it impersonated AP reporter in 2007 case, Associated Press, 7 Nov. 2014, http://www.chieftain.com/news/3043213-119/fbi-press-letter-comey.

[1313] See Eric Tucker, FBI leaves door open on agents' impersonating reporters, Associated Press, 9 Dec. 2014, http://www.seattletimes.com/seattle-news/fbi-leaves-door-open-on-agentsrsquo-impersonating-reporters/.

The FBI's impersonation of the Associated Press is the only example I know of where a law enforcement agency impersonated an innocent, trusted entity in an effort to deliver malware. There are, however, several examples of intelligence agencies engaging in similar tactics. For example, in 2012, researchers revealed that *Flame*, a sophisticated piece of malware, later revealed to be the work of the US and Israel,[1314] had spread by impersonating the software update service built into Microsoft's Windows operating system.[1315] One expert described the ability to successfully impersonate Microsoft as the "Holy Grail of malware writers."[1316]

By impersonating a trusted software security update mechanism, these governments risked harming global Internet cybersecurity by giving users a reason to doubt the safety of automatic software updates.[1317] There are strong parallels between the impersonation of a critical piece of cybersecurity infrastructure and the sham polio vaccination program established by the CIA in an attempt to locate Osama bin Laden.[1318] Whatever the possible intelligence value of that operation was more than outweighed by the catastrophic impact it had on legitimate polio vaccination efforts.[1319]

Recommendation: Government agencies engaged in hacking operations should be prohibited from impersonating trusted professions, including doctors, lawyers, journalists, and the clergy. They should also be prohibited from impersonating, via technical means, app stores and other critical cybersecurity infrastructure used by software companies to deliver security updates.

III. Bulk hacking and general warrants

In addition to the targeted delivery of malware to specific targets, the FBI has, since at least 2013, engaged in bulk hacking. In a number of operations targeting users of so called Dark Web forums, the FBI has attempted to deliver malware to every computer that visited a particular website or server. This method of malware delivery, referred to as a *watering hole attack* by computer security experts, raises a number of troubling issues, in addition to the more general policy issues associated with the use of malware by law enforcement.

[1314] *See* Ellen Nakashima,Greg Miller and Julie Tate, U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say, Washington Post, 19 June 2012, https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html.
[1315] *See* Dan Goodin, Flame malware hijacks Windows Update to spread from PC to PC, Ars Technica, 5 June 2012, http://arstechnica.com/security/2012/06/flame-malware-hijacks-windows-update-to-propogate/.
[1316] *See* Mikko Hyppönen, Microsoft Update and The Nightmare Scenario, F-Secure Labs, 4 June 2012, http://www.f-secure.com/weblog/archives/00002377.html.
[1317] *See* Christopher Soghoian, Lessons from the Bin Laden Raid and Cyberwar, Speech at Personal Democracy Forum, 11 June 2012, https://www.youtube.com/watch?v=swHkpHMVt3A.
[1318] *See* Donald G. McNeil Jr, C.I.A. Vaccine Ruse May Have Harmed the War on Polio, New York TImes, 9 July 2012, http://www.nytimes.com/2012/07/10/health/cia-vaccine-ruse-in-pakistan-may-have-harmed-polio-fight.html. After the CIA was criticized by the public health community, the agency promised not to make 'operational use' of immunization programs in the future. *See* Letter from Lisa O. Monaco, Assistant to the President for Homeland Security and Counterterrorism, 16 May, 2014, http://apps.washingtonpost.com/g/page/national/letter-to-deans-of-public-health-institutions/1040/.
[1319] *Id.*

In February 2015, the FBI launched a watering hole attack targeting visitors to Playpen, a child pornography forum only accessible via Tor.[1320] According to the FBI, the site had more than 214,000 registered users.[1321] Although the search warrant in this case remains sealed, the FBI's boilerplate warrant application for watering hole operations targeting Tor sites includes language requesting authority to deliver malware to "any user or administrator who logs into [the target website] by entering a username and password."[1322]

Even if the FBI was able to demonstrate probable cause that every single one of the 214,000 registered users of this website was violating the law, a single court order authorizing the government to hack into so many computers is no longer a search warrant, identifying places or persons to be searched, but a general warrant, authorizing the government to search the population of a decent sized city. Quite simply, there is no way for a single magistrate judge to engage in meaningful oversight of hacking at such scale, even more so when the computers of the targets are almost certainly located around the world.

That law enforcement officers can now hack 214,000 computers with the same effort as one or two computers is a testament to the power of modern technology and a stark reminder that the marginal cost of surveillance has plunged.[1323] As Judge Richard Posner observed a few years ago, "technological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive."[1324] However, just because law enforcement agencies are now capable of hacking at scale, doesn't automatically mean that they should be permitted to do so.

Recommendation: Bulk hacking operations and watering hole attacks should be prohibited.

IV. Bulk hacking and cloud computing

In August 2013, all of the websites hosted by Freedom Hosting—a service that hosted websites through the Tor network—began serving an error message to visitors with hidden code embedded in the web page.[1325] That code was specifically designed to exploit a security flaw in a version of the Firefox web browser used to access Tor hidden servers.[1326] According to an FBI agent who later testified in an Irish court, the Freedom Hosting service hosted at least 100 child pornography websites.[1327] But the service also hosted a number of legitimate sites, including *TorMail*, a web-based email service that could only be accessed over the Tor network, and *The Hidden Wiki*, which one news site described as the "de facto encyclopedia of the Dark Net." Even though these sites were serving lawful content, the

[1320] *See* Complaint in *United States v. Luis Escobosa*, Sept. 23 2015, page 6, https://regmedia.co.uk/2015/09/30/fbi_tor.pdf (revealing the website's name to be "Playpen")
[1321] *See* John Robertston, Special Agent, Federal Bureau of Investigation, Affidavit In Support of Application For A Search Warrant, 10 June 2015, page 7, https://assets.documentcloud.org/documents/2166606/ferrell-warrant-1.pdf
[1322] *See* Affidavit In Support of Application for Search Warrant (sample), pages 189-210 of http://www.uscourts.gov/file/15534/download at 200.
[1323] *See* Kevin S. Bankston & Ashkan Soltani, Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones, 123 Yale L.J. Online 335 (2014), http://www.yalelawjournal.org/pdf/1231_jjd1qz1e.pdf.
[1324] *See United States v. Garcia*, 474 F.3d 994, 998 (7th Cir. 2007).
[1325] *See* Kevin Poulsen, FBI Admits It Controlled Tor Servers Behind Mass Malware Attack, Wired, 13 Sept. 2013, http://www.wired.com/2013/09/freedom-hosting-fbi/.
[1326] *See* Dan Goodin, Attackers Wield Firefox Exploit to Uncloak Anonymous Tor Users, Ars Technica, 5 Aug. 2013, http://arstechnica.com/security/2013/08/attackers-wield-firefox-exploit-to-uncloak-anonymous-tor-users/.
[1327] Poulsen, FBI Admits It Controlled Tor Servers Behind Mass Malware Attack, *supra*.

FBI's watering hole attack was performed in an overbroad manner, delivering malware to visitors to all of the Freedom Hosting
sites, not just to visitors to those sites that were engaged in the distribution of illegal content.

We are now firmly in the age of cloud computing, in which hundreds of websites may share resources provided by the same powerful servers. Law-abiding Internet users have no way of knowing if the sites that they are visiting are hosted on the same physical server as a site that facilitates illegal conduct. That websites with a potential connection to illegal conduct are hosted on the same server as legitimate websites is not sufficient reason to permit law enforcement agencies to hack into the computers of every person who interacts with a particular server.

The court order that the FBI presumably obtained before launching watering hole attacks targeting the visitors to the many Freedom Hosting websites is not public. As such, it is impossible to know what the FBI agents told the court, or what the court authorized. We do not know if the judge authorized the FBI to deliver malware to all visitors to all sites running on the server owned by Freedom Hosting, or if the FBI agents exceeded the scope of the warrant. In any event, this episode demonstrates one of the major risks of bulk hacking and of the importance of strict limits on the use of such capabilities, particularly when targeting visitors to sites that are hosted in the cloud.

Recommendation: If bulk hacking operations are permitted, government agencies should be required to narrowly target their use of malware so that innocent persons who are visiting lawful, legitimate content on sites hosted on the same servers ("in the cloud") are not incidentally infected.

V. Law enforcement will increasingly need zero-day exploits to hack targets

The successful execution or installation of malware will generally require law enforcement to exploit a security vulnerability in the software on a target's computer. In order to do so, the target's computer must either be running out-of-date software with a known software vulnerability, or law enforcement must know of a so-called "zero-day" vulnerability for which no update exists.[1328]

Although some sophisticated targets may follow good information technology security practices by regularly updating their software, most people do not.[1329] As such, law

[1328] *See* Leyla Bilge & Tudor Dumitras, Before We Knew It: An Empirical Study of Zero-Day Attacks in the Real World, Proceedings of the 2012 ACM Conference on Computer and Communications Security, available at http://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf ("A zero-day attack is a cyber attack exploiting a vulnerability that has not been disclosed publicly. There is almost no defense against a zero-day attack: while the vulnerability remains unknown, the software affected cannot be patched and anti-virus products cannot detect the attack through signature-based scanning.").

[1329] *See* Thu Pham, Detecting Out of Date and Vulnerable Flash Versions on Your Network, Duo Security, 8 Oct. 2015, https://www.duosecurity.com/blog/detecting-out-of-date-and-vulnerable-flash-versions-on-your-network ("[W]e found that on average, 46 percent of corporate PCs are running out of date versions of browsers, Flash and Java. Users browsing on Safari and Internet Explorer were running out of date browser versions, at 61 and 57 percent, respectively….Our data

enforcement agencies have frequently been able to hack targets without needing zero-day security exploits.

Similarly, law enforcement agencies could, until recently, reliably hack large numbers of users visiting sites on the so-called Dark Web, without the aid of a zero-day exploit, because the Tor Browser did not include an automatic security update mechanism. For example, the FBI has on at least two occasions performed watering hole attacks which exploited flaws in the Tor Browser to identify visitors to child pornography sites.[1330] The malware used by the FBI in these operations did not work against the latest version of the Tor Browser, but the operations were still successful, as many visitors to the sites were running out of date, vulnerable software.

In August of this year, the Tor Project introduced a mechanism to deliver automatic updates to the Tor Browser.[1331] Over time, more and more users of Tor will be running a more recent version with automatic updates, which will mean that law enforcement operations against users of Tor will increasingly require a zero-day exploit. As such, if law enforcement agencies in the UK have not yet acquired and used zero-day exploits, I imagine that they will soon.

VI. Policy concerns associated with law enforcement use of zero-day exploits

There is no doubt that zero-day exploits will enable law enforcement agencies to more reliably hack the computers of targets, just as there is no doubt that nuclear weapons enable the military to more effectively kill its enemies. But both technologies have significant collateral costs which should give policy makers reason to limit, if not prohibit their use.

When a government acquires a zero-day exploit and decides to use it rather than notifying the company or developers responsible for the software, the government is, in essence, leaving all of its own citizens who use that software vulnerable, so that it may exploit the flaw against a small number of them later. By choosing to use, rather than disclose that flaw, the government is also gambling that no other party will independently discover and exploit the flaw. This is a big gamble to make, as security researchers frequently discover

found that 30 percent of users are running an out of date version of Flash, while 50 percent of users are running an out of date version of Java.")

[1330] *See* Kevin Poulsen, The FBI Used the Web's Favorite Hacking Tool to Unmask Tor Users, Wired, 16 Dec. 2014, http://www.wired.com/2014/12/fbi-metasploit-tor/ ("Only suspects using extremely old versions of Tor, or who took great pains to install the Flash plug-in against all advice, would have been vulnerable."). See also Kevin Poulsen, FBI Admits It Controlled Tor Servers Behind Mass Malware Attack, Sept 13 2013, http://www.wired.com/2013/09/freedom-hosting-fbi/ ("On August 4, all the sites hosted by Freedom Hosting...began serving an error message with hidden code embedded in the page….the code exploited a critical memory management vulnerability in Firefox that was publicly reported on June 25, and is fixed in the latest version of the browser….Tor Browser Bundle users who installed or manually updated after June 26 were safe from the exploit.").

[1331] *See* Mike Perry, Tor Browser 5.0 is released, 11 Aug, 2015, https://blog.torproject.org/blog/tor-browser-50-released ("Starting with this release, Tor Browser will now also download and apply upgrades in the background, to ensure that users upgrade quicker and with less interaction."). *See also* Tor Weekly News, 20 Aug. 2015, https://blog.torproject.org/blog/tor-weekly-news-%E2%80%94-august-20th-2015 ("The Tor Browser team put out a new stable version of the privacy-preserving browser….Thanks to the new automatic update mechanism in the Tor Browser 5.x series, you are probably already running the upgraded version!").

the same security flaws. One recent example of a high-profile flaw independently discovered by multiple research teams was the HeartBleed flaw in 2014.[1332]

Indeed, as ex-White House cyber czar Howard Schmidt observed in 2013, "It's pretty naïve to believe that with a newly discovered zero-day, you are the only one in the world that's discovered it...Whether it's another government, a researcher or someone else who sells exploits, you may have it by yourself for a few hours or for a few days, but you sure are not going to have it alone for long."[1333] In Schmidt's view, when governments exploit zero-day vulnerabilities rather than report them, "we all fundamentally become less secure.'"

In addition to the risk that another government, a researcher or cyber-criminal will independently rediscover the same vulnerability, every time a government uses a zero-day exploit, that government risks discovery, reuse and or disclosure of the exploit by the target, security researchers, cyber-criminals, or another government. This is because governments have no ability to control the redistribution of malware or software exploits that they have transmitted over the Internet to targets. As a result, the U.S. Department of Justice cautions its attorneys and agents about these specific risks:

> [O]nline undercover facilities that offer the public access to information or computer programs that may be used for illegal or harmful purposes may have greater capacity than similar physical-world undercover entities to cause unintended harm to unknown third parties. Because digital information *can be easily copied* and communicated, it is *difficult to control distribution* in an online operation and so limit the harm that may arise from the operation.[1334] (emphasis added)

This scenario is by no means theoretical.

The FBI's bulk hacking operation against visitors to Freedom Hosting in 2013, which I described earlier in this document, was quickly noticed by savvy users. Within days, the FBI's malware had been reverse-engineered by security researchers and the IP address of the FBI's server at a data center in Virginia had been identified.[1335] Although, as I described earlier, the FBI did not use a zero-day exploit in this case, had the agency used one, it would almost certainly have been discovered. According to one ex-law enforcement official, the FBI is apparently "loath to use [malware] when investigating hackers, out of fear the suspect

[1332] See Adriana Lee, How Codenomicon Found The Heartbleed Bug Now Plaguing The Internet, ReadWrite, 13 April 2014, http://readwrite.com/2014/04/13/heartbleed-security-codenomicon-discovery ("Discovered independently by Google engineer Neel Mehta and the Finnish security firm Codenomicon").
[1333] *See* Joseph Menn, U.S. Cyberwar Strategy Stokes Fear of Blowback, Reuters, 10 May 2013, http://www.reuters.com/article/2013/05/10/us-usa-cyberweapons-specialreport-idUSBRE9490EL20130510. *See also* Nicole Perlroth and David E. Sanger, Nations Buying as Hackers Sell Flaws in Computer Code, N.Y. Times, 13 July 2013, http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computerflaws.html.
[1334] *See* U.S. Department Of Justice, Online Investigative Principles for Federal Law Enforcement Agents, Nov. 1999, at 44 (p. 57 of the PDF) https://info.publicintelligence.net/DoJ-OnlineInvestigations.pdf.
[1335] *See* Vlad Tsyrklevich, untitled, Aug. 2013, https://tsyrklevich.net/tbb_payload.txt, ("this payload connects to 65.222.202.54:80 and sends it an HTTP request that includes the host name (via gethostname()) and the MAC address of the local host (via calling SendARP on gethostbyname()->h_addr_list). After that it cleans up the state and appears to deliberately crash.")

will discover and publicize the technique.[1336]" The Freedom Hosting operation and the subsequent discovery and analysis of the FBI's malware suggests that this fear is justified.

The *Stuxnet* worm, created by the United States and Israel, also serves as a good example that government malware and any associated zero-day vulnerabilities, may eventually be discovered. Although it took several years before Stuxnet was identified by security researchers, the Stuxnet code and the zero-day exploits it leveraged were extensively analyzed by a world-wide network of security experts.[1337] Once notified by the research community, Microsoft rushed to develop and distribute patches for these vulnerabilities. However, criminals also took note, and exploited the same vulnerabilities for their own nefarious purposes.[1338]

Recommendation: Law enforcement agency use of zero-day exploits should be prohibited. If the use of zero-days is permitted, a vulnerability equities process should be established to evaluate the risks associated with each particular vulnerability.[1339] Preferably, this process should be more transparent than the largely-secret process in use by the U.S. government.[1340]

VII. Conclusion

I appreciate the opportunity to present my views and policy recommendations on hacking by the government to this committee. Although my comments focus on this one topic, that I have not commented on the other parts of the Investigatory Powers Bill should in no way be interpreted as silent approval for the other surveillance powers that the government has sought. Given the extremely short window for public comments and the many problems associate with government hacking, I have not had the time to draft in-depth analysis and recommendations for the other parts of the bill. Should the committee have follow-up questions about government hacking or questions about any other part of the bill, please let me know, and I'd be happy to answer them.

Christopher Soghoian

[1336] *See* Jennifer Valentino-DeVries and Danny Yadron, FBI Taps Hacker Tactics to Spy on Suspects, Wall Street Journal, 3 Aug. 2013, http://www.wsj.com/articles/SB10001424127887323997004578641993388259674.

[1337] *See* David Kushner, The Real Story of Stuxnet, IEEE Spectrum, 26 Feb 2013, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

[1338] *See* Pierluigi Paganini, Kaspersky Revealed that Stuxnet Exploits Is Still Used Worldwide, Security Aff. 19 Aug. 2014, http://securityaffairs.co/wordpress/27633/cyber-crime/stuxnet-flaw-still-targeted.html.

[1339] *See* Kim Zetter, See U.S. Gov Insists It Doesn't Stockpile Zero-Day Exploits to Hack Enemies, Wired, 17 Nov. 2014, http://www.wired.com/2014/11/michael-daniel-no-zero-day-stockpile/ ("'the agencies that you would expect' use a 'multi-factor test' to examine vulnerabilities to determine how extensively the software is used in critical infrastructure and US government systems, and how likely it is that malicious actors have already got ahold of it or may get hold of it. 'All of those questions that are laid out, we require that analysis and discuss each one of those points. Then groups of subject-matter experts across the government make a recommendation to this interagency group that I chair here on the National Security Council.' The subject-matter experts provide 'their best judgment about [a vulnerability's] widespreadness or how likely it is that researchers are going to be able to discover it or how unlikely it is that a foreign adversary has it.'")(Quoting White House "cyber czar" Michael Daniel, describing the White House Vulnerability Equities Process)

[1340] *See* Andrew Crocker, The Government Says It Has a Policy on Disclosing Zero-Days, But Where Are the Documents to Prove It?, EFF Deep Link Blog, 30 Mar. 2015, https://www.eff.org/deeplinks/2015/03/government-says-it-has-policy-disclosing-zero-days-where-are-documents-prove-it. *See also* Andrew Crocker, It's No Secret That the Government Uses Zero Days for "Offense", EFF Deep Links Blog, 9 Nov. 2015, https://www.eff.org/deeplinks/2015/11/its-no-secret-government-uses-zero-days-offense.

Dr. Christopher Soghoian—written evidence (IPB0167)

21 December 2015

Giuseppe Sollazzo—written evidence (IPB0032)

1. Executive Summary

The Investigatory Powers Bill introduces concepts of bulk collection and storage of personal communications data that are problematic under many aspects.

My comments to the bill follow my previous written submission. These come under three points which cover broadly the three thematic areas, but focus specifically on three technical aspects in the context of interception and communication data storage:

a) technical misunderstandings regarding how encryption works, and how it can be used without need for a central infrastructure. Encryption neither works in the way the bill presumes it does, nor it is used in the purported way; specifically, it can be used point-to-point, bypassing the ISPs

b) issues regarding due legal process, based on a judicial review. Judicial approval of warrant would be a more adequate system with the right safeguards.

c) practical considerations of applicability of the bill, if passed into law. The system envisioned by the bill does not likely improves security against terrorism or serious crime.

2. Personal Profile

I am a Senior Systems Analyst at St George's, University of London with 10 years of experience in IT, especially in the management of confidential, health-related, databases. I am currently a member of the advisory Technical Standards Board at Cabinet Office. I have been a member of the Open Data User Group, always at Cabinet Office (2013-2015), and of the Health and Social Care Transparency Panel at the Department of Health (2014-2015). I am also link School Governor on Freedom of Information and Data Protection.

3. Extended Submission

3.1 Technical issues

The bill introduces the requirement for ISPs/technical companies to weaken encryption algorithms on demand to allow wiretapping by security agencies.

This requirement is based on two major misunderstandings:

a) how encryption works, i.e. a mathematical procedure and its technological implementation in a software programme; the mathematics cannot be broken, while the implementation can and this introduces security risks rather than addressing them

b) the fact that a vanilla, non-weakened version of the algorithm could be used in a point-to-point, peer-to-peer fashion, bypassing the ISPs; this is not just technically feasible but also very simple.

3.1.1 Explanation of why encryption is secure

Any encryption system is based on two key concepts: a mathematical procedure, and its implementation. The form of encryption most frequently used on the Internet today is called public-key cryptography and the most common algorithm used is RSA.

The maths on which RSA is based is beautifully simple, and quite strong. The proof of correctness for RSA amounts to a handful of lines based on very simple algebra. In other words, unless we are very wrong on something very fundamental, it is extremely unlikely that the maths behind RSA can be broken.

3.1.2 Security flaws introduced in the implementation increase risks

This means that the Government is asking ISP and technical companies to deliberately add bugs in the *implementation* of such algorithms as they are used on the web. The dangers of this are self-evident: once a broken implementation is in use, it's in use for everyone, including the very people against which the bill is trying to protect the public.

As Tim Cook, Apple's CEO, eloquently puts it:
"Any back door is a back door for everyone. Everybody wants to crack down on terrorists. Everybody wants to be secure. The question is how. Opening a back-door can have very dire consequences.
If you halt or weaken encryption, the people that you hurt are not the folks that want to do bad things. It's the good people. The other people know where to go."

Encryption software cannot be weaken in a "controlled" way. If a flaw is added, this might be revealed by a whistleblower or, most likely, hackers will find it by themselves.
Weakening security does just that: it weakens everyone's security; our own security, the Government's security, society's security.
If details of the security backdoor are publicised and hackers get hold of it, our credit cards are at risk; our bank accounts are at risk; our e-mails are at risk. If the hackers are ISIS terrorists, we might be helping them access sensitive details with even more ease than before.

3.1.3 Encryption can be used point-to-point, bypassing the ISPs

The second point, however, is what I find most troubling. It shows that the bill is *misunderstanding what encryption is and how it can be used*.

The bill assumes that all communications pass through ISPs or telecoms providers, who can act on the encrypted communications channel. However, the *content* of the communication channel can be encrypted itself in a relatively straightforward way: public-key algorithms can be used to encrypt messages without any need of support from a service provider. Once the two people involved have exchange cryptographic keys, they can use them to encrypt messages sent over the standard communication channels, with no way for the ISPs to break that encryption. It would not be just difficult: it's mathematically impossible.

The bill also underestimates the ease with which this can be done. Anyone with little computing knowledge can write their own implementation on a computer, and use it. Terrorists can exchange cryptographic keys in any way (including by writing them down on a

piece of paper) and write their own programme to encrypt and decrypt messages. A simple implementation of RSA is just 20 lines of code.

Once they have it, they can simply send their messages on any system; the messages will be encrypted in an unbreakable way. Although the network could theoretically *detect* that an encrypted message has been sent, no one would be able to decrypt it. The backdoor cannot be added to a self-developed implementation of a public-key encryption system, and outlawing the use of maths sounds surreal. The bill confuses between services and algorithms, and it does so in a terribly dangerous way.

3.1.4 Consequences to consumers

The requirement for ISPs to weaken encryption while keeping logs of user activity for 12 months is, other than unethical, potentially dangerous and daunting for consumers. Keeping logs is not just expensive to the ISPs, resulting in likely increases in broadband bills, but could also have dire consequences, as in the recent data hacking of TalkTalk: how much more dangerous could have the hacking been, had the hackers found data for the previous 12 months, rather than 2–3? Such amounts of data cannot be stored in a way that is 100% secure, and not certainly economically.

3.2 Problems around the legal process

The legal authorisation process proposed by the bill contains some worrying points. This is based on a judicial review, which would allow the Home Secretary to authorise a warrant without involvement of judges. A judicial review is simply a post-mortem verification that the correct *procedure* was followed. It is not an analysis of evidence and facts.
Hence, if the Secretary of State has authorised a warrant with no evidence or facts, but has done so respecting the procedure, the review will return a positive result. Two separate reports commissioned by the Government recommended that authorisation should come from the judiciary. Judicial authorisation is generally a good idea that prevents abuse and introduces the right safeguards.

3.3 Practical considerations

The final point I would like to make is that the bill would hardly be practical. This is not a mundane question, and has been asked, among others, by the Financial Times [http://blogs.ft.com/david-allen-green/2015/11/05/the-investigatory-powers-bill-will-it-work-in-practice].

Will the powers of mass data logging allow better detection of terrorism? As we have learned from the Paris attacks, there was no lack of surveillance: many of the attackers were known to police. However, police had not enough resources to follow all the leads.
Huge amounts of data might be completely useless. Terrorist activity is not necessarily something that a smart algorithm can magically "detect". Terrorists might not even have to communicate online in order to arrange an attack like the deadly Bataclan mass-murder.

Reports from "Le Monde" [http://www.lemonde.fr/attaques-a-paris/article/2015/11/18/le-telephone-portable-d-un-membre-du-commando-trouve-pres-du-bataclan-a-permis-de-remonter-a-alfortville_4812515_4809495.html] suggest that the attack was initiated minutes before by SMS (unencrypted). Mass data logging would have not helped.

As Bruce Schneier, the world's most famous computer security expert, puts it
"Finding terrorism plots is not a problem that lends itself to data mining. It's a needle-in-a-haystack problem, and throwing more hay on the pile doesn't make that problem any easier."
Investing in human intelligence and police resources might be a more sensible approach.

4. Conclusions

As illustrated, the bill is based on flawed technical assumptions and a doubtful legal process. I would argue that a total rethink of what the bill is trying to achieve is needed, in consultation with independent technical experts.

17 December 2015

TalkTalk—written evidence (IPB0154)

A. About TalkTalk

A.1 TalkTalk entered the market in 2006 with the aim of democratising telecoms. Today, TalkTalk is the UK's challenger telecoms company, providing landline, broadband, TV and mobile services to over 4 million customers. We operate Britain's biggest unbundled broadband network, covering 96% of the population, supplying services to consumers through the TalkTalk brand and to businesses through TalkTalk Business and by wholesaling to resellers.

A.2 TalkTalk welcomes the Committee's scrutiny of the draft Investigatory Powers Bill and the opportunity to submit written evidence.

B. TalkTalk's approach

B.1 TalkTalk supports the Government's desire to update and consolidate relevant investigatory powers into a single Act. At present, the laws governing investigatory powers and data retention requirements are contained in disparate pieces of legislation, some of which will expire later this year. The Government is right to take the opportunity to simplify the legislation, bringing the various powers into a single Act. Doing so presents an opportunity to increase transparency and strengthen oversight arrangements.

B.2 TalkTalk considers it a matter for Parliament to determine the appropriate balance between liberty and security. In consultation with Government on the Bill, and for the purposes of this submission, we have attempted to restrict our comments to improving the effectiveness of the legislation as opposed to expressing a view on the principles of it.

B.3 It is worth noting that important details of how the investigatory powers system will operate are not defined in the draft Bill. The Government has indicated that secondary legislation and Codes of Practice will set out the exact definitions and interpretations of issues such as internet connection records, and how the system will account for the limitations in their use caused by proxy servers and virtual private networks. It is vital any secondary legislation or Codes of Practice are effectively scrutinised.

C. Judicial oversight

C.1 TalkTalk welcomes the oversight role of the Investigatory Powers Commissioner (IPC) and judicial commissioners. The 'double lock' is essential to building public confidence in the data retention and investigatory powers system.

C.2 We recognise that there may be a limited number of urgent cases where pre-emptive judicial oversight is not possible. We believe the exemption system outlined in the draft Bill strikes a broadly appropriate balance between the need for swift action by the police and security services and the need for judicial oversight. We welcome the fact that the annual IPC report will be made public and consider it important that the report details the number of times where judicial oversight was sought retrospectively.

C.3 We welcome the consolidation of the existing oversight bodies into a new, single organisation. We note that under the current draft Bill, retained data infrastructure security would fall outside the remit of the new body. There may be a case for considering whether oversight would function more effectively by correcting this anomaly.

D. Implementation

D.1 We note that the timeline for the Bill is driven in part by the sunset clause on the Data Retention and Investigatory Powers Act 2014.

D.2 Whilst we welcome the desire to ensure that the new legislative framework is agreed prior to December 2016, elements of the draft Bill involve significant operational and technical challenges for CSPs. For instance, proposals on internet connection records would require significantly expanded processing, network and storage infrastructure, as well as software developments to define and implement new systems. This is likely to take several years to implement in full. It is therefore essential that the implementation timeline takes account of those challenges.

D.3 We welcome the consultative approach the Government has taken in preparing the draft Bill. We will continue to work with Government to ensure the technical challenges are fully understood and that an appropriate implementation timeline is agreed.

E. Third party data retention

E.1 The Home Secretary has stated that unlike the draft Communications Data Bill 2012, this Bill will not require CSPs to retain third party data. Speaking in the House of Commons on 4th November, the Home Secretary said: “Let me be clear: the draft Bill we are publishing today is not a return to the draft Communications Data Bill of 2012. It will not include powers to force UK companies to capture and retain third party internet traffic from companies based overseas”.

E.2 TalkTalk welcomes the exclusion of third party data requirements. The draft Bill, however, would benefit from greater clarity on this point. Clause 71(9) should be modified to make clear that ‘relevant communications data’ exclusively relates to data generated on a CSP’s own network, or data processed by that operator in order to provide a service. This would distinguish it from transit data that may use a CSP network, but is of no relevance to a CSP.

F. Subject Access Request

F.1 Section 7 of the Data Protection Act 1998 allows individuals to request a copy of information an organisations hold about them, commonly referred to as a subject access request.

F.2 The draft Bill would significantly expand the volume of data CSPs are required to retain. It is therefore critical that careful consideration is given to how subject access requests would apply to the new information. If all customer data, including internet connection records, could be requested, CSPs would face significant challenges delivering the sheer volume of data to customers in a safe, practical way.

F.3 Privacy issues must also be carefully considered, as the data would relate to each individual who has used an internet connection, not just the account holder. In the case of an internet connection record, this would allow customers to potentially see data relating to the browsing habits of a spouse or housemate, which has significant privacy implications.

F.4 Careful consideration should be given to whether all additional data CSPs are required to retain should be subject to subject access requests.

G. Cost recovery

G.1 The draft Bill includes measures to increase CSP retention requirements. For instance, CSPs would be mandated to retain internet connection records for 12 months. Retaining this data, and storing it securely, represents a significant new cost for CSPs.

G.2 Whilst the Government has indicated that it accepts the principle of cost recovery (i.e. that the Government reimburses CSPs for costs associated with the data retention requirements in the Bill), these arrangements should be more explicitly outlined in the Bill to provide taxpayers and CSPs with greater clarity about how the cost recovery model will work. Without an effective and clearly defined cost recovery model, consumers face the very real risk of seeing their bills rise to pay for the implementation of the Bill.

8 January 2016

techUK—written evidence (IPB0088)

About techUK

1. techUK represents the companies and technologies that are defining today the world that we will live in tomorrow. More than 850 companies are members of techUK. Collectively they employ approximately 700,000 people, about half of all tech sector jobs in the UK. These companies range from leading FTSE 100 companies to new innovative start-ups. The majority of our members are small and medium sized businesses.

Introduction

2. The Government's draft Investigatory Powers Bill, which will provide provisions for the interception of communications, the retention and acquisition of communications data, the use of equipment interference and the acquisition of bulk data for analysis, has correctly been described by the Prime Minister as "one of the most important pieces of legislation in this Parliament".

3. techUK wholeheartedly supports the parliamentary process that has been conducted to date and welcomes the attempt to bring authorised surveillance powers under one single piece of legislation. The draft Bill must be worthy of emulation around the world by setting high standards of privacy protection for users and, if copied by other Governments, can be the cornerstone of an international framework that is transparent, workable and predictable for global companies, agencies and citizens.

4. Whilst the safeguards proposed in the draft Bill aim to be specific and precise, the powers the draft Bill affords to the security services remain broad and create a number of concerns for techUK members. For this reason, it is crucial that the Joint Committee is afforded sufficient time to properly scrutinise the draft Bill in order to assess its effect on citizens, consumers and implications for the UK's digital economy.

5. In particular, the Committee should pay close attention to the necessity and proportionality of many of the provisions within the draft Bill; the clarity that the draft Bill gives to the technology sector; and the future potential use and implications of the powers proposed. The rapid evolution of the technology sector means that the key tests to apply when scrutinising the draft Bill are not whether certain requirements are technically feasible today, but whether those requirements will stand the test of necessity and proportionality as technology changes. The Committee must also consider whether the steps taken to fulfil those requirements - in terms of time, cost (including opportunity cost), knock-on effects and change in customer relationships - are reasonable and proportionate to the expected benefits.

6. techUK has set out below some key issues that are of upmost importance to techUK members including:

- Greater clarity on new powers afforded in the Bill and the extension of current powers

- Clearer definitions of terms used within the draft Bill
- Extra-territorial application of most powers
- Further clarification on encryption and bulk equipment interference

1. Analysis of new and extended powers proposed in the draft Bill

7. One of the most significant new powers proposed in the draft Bill is the extension of the definition of types of "communications data" that CSPs are required to retain to include what the Government has called "internet connection records" (ICR).

Definition of Internet Connection Records is unclear and inconsistent

8. ICRs are defined in the 'Guide to Powers and Safeguards' to the draft Bill as "a record of the internet services a device has connected to, like a website or messaging application". Clause 47(6) elaborates on this definition further, and defines ICRs as data which "may be used to identify a telecommunications service to which a communication is transmitted through a telecommunication system for the purpose of obtaining access to, or running, a computer file or computer program" and data that is "generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication (whether or not a person)". According to the 'Factsheet' on ICRs that was published alongside the draft Bill, the retention of ICRs will enable the security services to "see that a person has used google.co.uk or facebook.com" but not "what searches have been made on google or whose profiles had been viewed on Facebook".

9. It should be noted that Clause 47(6) is the only reference to ICRs in the draft Bill and the retention powers contained in Clause 71 do not explicitly mention ICRs. In fact the draft Bill contains two different provisions, in Clause 47 and Clause 71, which the Explanatory Notes say are meant to describe ICRs. Whilst one describes "data which may be used to identify a telecommunications service" (Clause 47(6)), the other definition relates to "communications data which may be used to identify…the internet protocol address or other identifier of…apparatus". The lack of clarity and confusion in the draft Bill as to the actual definition of an ICR exemplifies the fact that ICRs are completely new types of data that do not match actual data types processed, generated or stored by companies for general business purposes.

Generation of Internet Connection Records will be difficult

10. Requiring the retention of ICRs represents a significant change for companies, changing the operational process in how companies retains data. Some internet service providers may face technical difficulties in separating the first part of the URL up to the first "/" (classified as communications data by the draft Bill and required) from the remainder of the URL after the first "/" (classified as communications content and not required).

11. Similar concerns over the difficulty of generating ICRs exist due to the definitions of what constitute, and difficulties in separating, "communications data" and "communications content". The definition of "communications data" relates to the "who, what, where, when and with whom" of a communication, yet does not appreciate the vast amounts of metadata that companies would have to retain under the requirements of the draft Bill and the difficulty for companies in separating data (which can be accessed without a warrant) from content (which could not be accessed without a warrant). The extent to which the two can be easily separated requires greater scrutiny – clearer definitions, and acknowledgement of, the metadata in between is therefore required.

Internet Connection Records will contain highly sensitive data and will need to be kept secure

12. The magnitude of data processed and the security of the retained ICRs must be properly understood, since access to such records by malicious actors can be even more dangerous than other types of communications data. This is due to the vast amounts of data that will end up being retained and the inferences about people's activities, political views, sexual orientation and interests that such data can reveal. Businesses may also need to build and maintain specific infrastructure to ensure that the data retained is secure.

Questions on the usefulness of Internet Connection Records

13. Furthermore, the Joint Committee must also consider whether the operational case made for ICRs justifies the need for them to be retained. The oft cited case made by the Home Office, of the use of ICRs by the police to know whether a missing person has accessed a social media app, has significant flaws and does not take into account the dynamic manner in which the internet works. Most mobile phones are connected to such apps throughout the course of the day. Therefore the usefulness of the ability of an ICR to record "the fact that a smartphone had accessed a particular social media website at a particular time", as stated by the Home Office, is questionable.

14. Recent evidence from Denmark, where a similar session logging data retention scheme operated from 2007-2014, also suggests that the retention of ICRs lacks effectiveness and fails to pass the test of necessity and proportionality. A Danish Ministry of Justice report into data retention showed that data from the session logging regime had only been used in a limited number of cases, and was especially difficult for law enforcement to make use of due to the vast amounts of data that was retained.

Costs of retaining Internet Connection Records should be fully reimbursed as a check to ensure proportionality

15. The implications of the proposals in the draft Bill on ICRs will differ between companies based on size, date of entrance into the market and current capabilities.

16. Nevertheless, requiring the retention of ICRs is a significant change for internet service providers and will add additional operational costs due to the vast amounts of data that passes through the internet on a daily basis. Although the draft Bill states that companies must receive "an appropriate contribution" towards the costs of complying with the Bill, and that the Government has set aside £175m towards the costs of retaining ICRs, it is unclear as to whether this figure will also relate to the costs of securing the retained data.

17. The Committee may also wish to consider whether the figure of £175m put towards the costs of retaining ICRs is a limit or a benchmark. In evidence to the Joint Committee in early December, Home Office officials claimed that the figure was "an estimate". The draft Bill does not definitively state whether the costs for retaining data will be fully reimbursed by Government, merely that the Government will make "an appropriate contribution" to the costs of retaining data that companies would not normally retain for business purposes.

18. The issue of costs is important, since it introduces an element of proportionality as to why a certain provision is required. If the estimate made by the Home Office as to the costs of retaining ICRs turns out to be far too small, then this would again raise the question of whether ICRs are necessary and proportionate. If Government is made responsible for meeting the full costs, this would provide an important check to ensure that the powers the Government seek to implement are proportionate. Furthermore, due to the uncertainty about the extent of the definition of ICRs and the extension of communication service providers that will be affected by the proposed provision, it becomes difficult to determine whether or not the estimate can be an accurate figure. The draft Bill should therefore make an explicit provision that Government would seek to reimburse industry the full costs of retaining such data, if required to do so.

19. It is a common misconception, frequently stated by the Home Office, that the retention of ICRs is the only new power in the draft Bill. This, however, is not the case.

"Relevant Communications Data" constitute more than Internet Connection Records

20. Clause 71 of the draft Bill lists the types of "relevant communications data" that must be retained by companies when issued with a data retention notice. This list includes a wider range of communications data than is currently on the list of retainable communications data provided for under current legislation, even when one takes into account the new provision on internet connection records.

21. "Relevant communications data" covers any type of communication on a network and internet connection. It is not limited to internet access, email or telephony and explicitly includes communications without human intervention, where the sender and recipient are machines. This therefore could include background interactions

that apps make automatically with their supplier servers. This wide definition highlights the inconsistency between the scope of retention explained in the 'Guide to Powers and Safeguards' and the scope of data retention empowered by the term "relevant communications data".

22. As stated above, it is important that the future scope of the powers proposed in the draft Bill are properly understood whilst the Bill is being scrutinized. In particular, how does the wider definition of "relevant communications data" affect the growing use of Internet of Things (IoT) devices and the machine-to-machine interaction that arises from IoT?

Data generation obligations – another new power

23. Current legislation requires CSPs to retain data that is, or will be, generated in the UK for business purposes. The draft Bill, however, extends this obligation by compelling companies to generate data that they otherwise would not have done in the course of providing its service.

24. Clause 71(8)(b), under powers to require retention of certain data, makes mention to the obtaining of data whether by "collection, generation or otherwise". This suggests that the Government reserves the right to compel companies to change their business models in order to facilitate access to data that they would not have kept under standard business operations.

25. Furthermore, the definition of "relevant communications data" is no longer limited to data processed by a company in its normal course of business but creates an additional obligation on CSPs to generate new types of data specifically for law enforcement purposes. So, for example, a CSP may be required to generate data about the location of its users and then store that date purely for the purposes of law enforcement.

26. This would appear to be a direct conflict with data protection obligations derived from EU Data Protection Law, including a revised directly applicable Regulation which was finalised by negotiators only on 15 December and which will come into effect one year after the investigatory Powers Bill is intended to have effect. There is no exemption in the Regulation for this type of requirement on companies to create and retain data that would not otherwise arise in the context of their activities. In fact the reverse is the case.

Extra-territorial proposals in the draft Bill remain unworkable

27. Communications and internet businesses have become more global in their structure and commercial operation. Users use a range of services, at times simultaneously, provided both in their home country and beyond. Agencies themselves now operate in a more global way, and increasingly request access to data in other jurisdictions and engage in joint investigations with agencies overseas.

28. It is therefore important that the draft Bill complements rather than conflicts with the international legal framework for the lawful acquisition of data by government agencies. It also needs to plot a path to addressing the gaps and conflicts which currently exist between jurisdictions rather than add to this complexity. This places greater importance on governments working together to build a coherent legal framework combining domestic legislation and appropriate international legal instruments which provide for the lawful acquisition of data from overseas.

29. Sir Nigel Sheinwald acted as the Prime Minister's special envoy on matters of jurisdiction and, in his review on law enforcement data sharing, he highlighted that the only long term solution to the current situation where data travels freely across natural borders is through an international legal framework that takes into account issues of proportionality, necessity and transparency. This framework must set clear, transparent guidelines that can serve as a model around the world that domestic surveillance laws should not unilaterally over-reach and limit the sovereign rights of other countries.

30. Despite Sheinwald's recommendations, extra-territorial provisions in the draft Bill remain for targeted interception warrants and mutual assistance warrants (S.29(4)); communications data acquisition notices (S.69(3)); targeted equipment interference warrants (S.99(3)); bulk interception warrants (S.116(3)); bulk acquisition warrants (S.130(3)); bulk equipment interference warrants (S.145(3)); technical capability notices (S.189(8)).

31. Whilst techUK members welcome provisions in the Bill to enable future international agreements and modernised mutual legal assistance mechanisms, it is worrying that seven out of the eight major powers in the draft Bill still have extra-territorial reach with inconsistent protections around reasonableness and conflicts of law, as well as enforcement.

32. There is strong anecdotal evidence showing that many governments – often in countries with immature democratic and human rights standards – are eagerly awaiting the Investigatory Powers Bill and have plans to propose similar laws. If the domestic legislation of other countries mirrored the extra-territorial powers in the draft Bill in its current form it would result in a patchwork of overlapping and conflicting laws around the world. This would create additional risks for businesses and of UK commercial interests, as well as impair the free flow of data to support the digital economy.

33. It is crucial that Parliament considers the domestic and international ramifications of the very broad territorial reach of the Bill as currently drafted. techUK believes there is a leadership opportunity for the UK government to lead government to government engagement with a view to modernising the international legal framework which has not kept pace with the complexities of international communications business, use and abuse.

2. The technical feasibility and proportionality obligations proposed in the draft Bill

34. The question of whether the provisions in the draft Bill are technically feasible and proportionate should not just focus on the implications of the draft Bill on technology today, but its use in the future as technology evolves.

Proposals on Equipment Interference threaten the security of the internet

35. The proposals in the draft Bill for a more explicit equipment interference regime must therefore take into consideration its future implications on the security of connected devices and the advent of the Internet of Things (IoT), particularly in relation to the use of bulk equipment interference.

36. Within the draft Bill, the term "equipment" is defined as any equipment "producing electromagnetic, acoustic or other emissions or any device capable of being used in connection with such equipment". This definition of equipment is hugely important as we move beyond a world that is just about telephony and accessing messaging services. This definition appears to apply to a huge range of devices that could be used for a whole range of purposes other than traditional means of communication, including devices that relay messages between non-human beings; i.e. machine-to-machine communications. From credit card payment systems to driverless cars, more and more connected devices rely on the internet and therefore could be made subject to bulk equipment interference.

37. The security implications of this broad definition requires careful scrutiny to determine its appropriateness, necessity and proportionality. Equipment interference, particularly in bulk, has the potential to affect innocent users and cause harm to the essential infrastructure that the digital economy relies on to thrive. This becomes even more concerning when one takes into consideration the fact that the draft Bill also sets out the guidelines in which companies are obliged to "take all steps to give effect" to an Equipment Interference warrant. Although the Bill caveats this by stating that companies should not be required to take steps that are not "reasonably practicable", legitimate questions arise on the exact obligations that companies will now face in giving effect to an Equipment Interference warrant in practice.

38. Whilst the provision for a legal basis for the authorities to seek to exploit vulnerabilities in devices for targeted investigative purposes is well understood, it is an entirely different matter to insist that companies are legally required to assist in these measures. This also creates questions in relation to liabilities that could arise for such service providers on an extra-territorial basis.

39. The reputational damage that could face a company that has to comply and assist with a bulk Equipment Interference warrant, thereby undermining the security of their services in bulk, is huge. The relationship between techUK members and their customers rests to a large degree on trust, and the 'contract' between them will be undermined if the businesses are made into an extension of intelligence agencies.

40. The situation is perhaps most acute for companies that rely on the support of the open source community, where their code has to be out and available in the public domain. Such companies would face considerable difficulty in meeting any bulk Equipment Interference requirements as they would not be able to conceal the requirements of the warrant from the open source community it relies on to operate.
41. The Joint Committee may therefore wish to consider the appropriateness of a provision that appears to place an obligation on companies to assist in the interference of their own equipment and thereby create vulnerabilities that could be exploited by others.

42. As the Government has now for the first time stated its intention to reflect in legislation the practice of exploiting or otherwise creating vulnerabilities to interfere with equipment, there is by necessity a corollary public interest obligation to bring such vulnerabilities to the attention of the relevant providers in a timely manner. It cannot be the case that Government can create an environment in which it becomes aware of vulnerabilities and can sit on them for an extended period with the clear understanding that the same vulnerabilities could be exploited by bad actors for reasons contrary to the interests of the UK public and economy.

43. Robert Hannigan of GCHQ has stated publicly that "In the last two years, GCHQ has disclosed vulnerabilities in every major mobile and desktop platform, including the big names that underpin British business. Vendors sometimes publicly credit (GCHQ) with finding those weaknesses." It is unclear how many of these disclosures GCHQ has made but the practice would seem to be in conflict with the intelligence agencies' simultaneous practice of equipment interference. It would be very helpful to the industry to understand how these two objective will work together.

Proposals on encryption remain unclear

44. The Committee may also wish to consider the effect such a requirement may have on the use of encryption by service providers, as the draft Bill could be interpreted as giving the Government the power to request companies to compromise their software in order to make encryption less secure in order to give an effect to a warrant. Although the Government has been at pains to stress that it is not restricting or weakening encryption, and that all requirements in the Bill regarding the "removal of electronic protection" are already provided for in current legislation, further scrutiny around this is needed in the light of the importance of encryption to building trust and confidence in the digital economy.

45. In particular it still remains unclear as to whether the obligation for service providers "relating to the removal of electronic protection", as stated in Clause 189(4)(c), has any ramifications for encryption technology applied by the user of the services, and not the service provider. If the provision does have ramification for end to end encryption, this would limit companies' ability to deploy the necessary security to safeguard their customers' privacy and security, in effect compelling companies to

weaken the security of their products. This would conflict with the legal obligations providers have to protect user data from unauthorised intrusion (ePrivacy Directive, Data Protection Directive, forthcoming Network and Information Security Directive).

46. Indeed it could result in companies being forced to replace products, since an end-to-end encrypted service in which the encryption is done at the device level is a different product to one in which the encryption is applied by the service provider, who then holds the keys. Importantly, this would often need to be done at a global level. Such a requirement would hinder innovation and create an unfavourable business environment in which widely used security technology is restricted.

47. This needs to be reconciled with Government policy on cybersecurity[1341]. For example, Baroness Shields (The Parliamentary Under-Secretary of State for the Department for Culture, Media and Sport) has previously stated in Parliament that the Government "recognise the essential role that strong encryption plays in enabling the protection of sensitive personal data and securing online communications and transactions… (and)…do not advocate or require the provision of a back-door key or support arbitrarily weakening the security of internet applications and services".[1342] The draft Bill should contain statutory provisions to require that the operation of investigatory powers under the Bill safeguard network integrity and cybersecurity.

48. It should be noted that Clause 190 states that the Secretary of State, before giving a notice relating to the removal of electronic protection, would have to consider the "technical feasibility" of complying with such a notice. For the test of whether a measure is "technically feasible" to be meaningful, it must consider something more than whether the end result is technically achievable with sufficient engineering manpower, investment and time. As stated above, the consideration as to whether a measure is technically feasible should also consider whether the time, cost (including opportunity cost), knock-on effects and change in customer relationships are reasonable and proportionate to the expected benefits.

Proposals on bulk collection need to be properly debated and scrutinised due to the high level of intrusiveness

49. The draft Bill includes a public avowal, for the first time, of the security services' bulk collection powers. Although current legislation provides for the acquisition of data in bulk, the draft Bill puts on a statutory footing all of the bulk powers available to the security services. The draft Bill also includes, in Clause 106(8), a new power for the security services to be able to extract and examine communications data derived from bulk intercepted content.

50. Once again, warrants for bulk collection will need to be approved (but not authorised) by a Judicial Commissioner before coming into force. Unlike previous

[1341] For further information, please see: http://www.theguardian.com/technology/2015/nov/09/tech-firms-snoopers-charter-end-strong-encryption-britain-ip-bill
[1342] House of Lords Debate, 'Cybersecurity: Encryption', 2015

legislation, which sought to distinguish between internal and external communications, the bulk regime in the draft Bill relates to communications 'sent by individuals' or 'received by individuals' outside the British Islands.

51. Furthermore, in relation to warrants that affect overseas operators, the Secretary of State authorising the warrant must not only consult the operator affected but also take into account the likely number of users that may be affected, the technical feasibility and likely cost of complying with any requirement that may be imposed on a company. The Explanatory Notes supporting the draft Bill make it clear that any costs incurred by a company in complying will be reimbursed by the State, but it remains important to understand the scope and scale of such requests.

52. As techUK has previously stated in the past, any provisions related to bulk collection powers have to account of the high levels of intrusiveness such powers bring with them and an appropriate level of checks and balances to reflect this. It should be noted that Parliament has not yet had the chance to debate the necessity and proportionality of bulk collection powers, unlike in the US where use of bulk data collection powers under Section 215 of the Patriot Act were debated at length in Congress and scaled back.

53. It is important that the Joint Committee critically examines the operational case put forward in the draft Bill for bulk collection in order to ensure that the capability is proportionate, necessary and effective.

3. Transparency

54. Since 2010 there has been growing public concern into how surveillance is conducted in the UK, with recent surveys revealing that 72% of British consumers are concerned about their private information online.

55. Small shifts in public sentiment regarding the security and privacy of users' communications can have serious consequences for the UK's digital economy. This is why many companies publish transparency reports for consumers – ensuring that citizens are fully informed of issues related to surveillance and privacy.

56. These concerns, as stated David Anderson QC (the Independent Reviewer of Terrorism Legislation), must be addressed in the draft Bill and considered by the Joint Committee. This includes more clarity in the definitions of the terms used in the draft Bill in relation to private networks, strengthened oversight and authorisation, greater transparency around the mechanisms for interception and the ability for companies to notify their users of the extent of data requests made to them.

Lack of clarity around private networks in the draft Bill harm transparency

57. It has been Government policy to keep the definitions of "telecommunications provider" and "telecommunications service" in the draft Bill deliberately broad in order to "future proof" the draft Bill.

58. The Data Retention and Investigatory Powers Act 2014 (DRIPA) first extended the definition of "public telecommunications operator" as being any company that provides a telecommunications service. In previous legislation (Regulation of Investigatory Powers Bill 2000), "telecommunications service" was defined as "any service that consists in the provision of access to, and of facilities for making use of, a telecommunications system". DRIPA, and the draft Investigatory Powers Bill, amend the meaning of "telecommunications service" to include any service which "consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of such a system".

59. The Government has maintained that the extension of the definition is to include internet based services, such as webmail. Yet since the draft Bill drops the use of the word "public", this means that various aspects of legislation that currently only apply to public services can now be extended to private services, including private company networks and private cloud services.

60. This raises a number of technical questions that the Committee may wish to consider. Would, for example, a hotel or University campus that offers network connections to customers and students be within the scope of the legislation? Whilst the necessity and proportionality tests in the legislation can understandably be applied to where companies provide public networks, it is less clear what the implications are for private company networks.

61. Applying the provisions in the draft Bill to private networks is unnecessary, disproportionate and would be detrimental to business network user confidence and transparency. The draft Bill should make it explicit that its provisions apply to "public telecommunications only", which would maintain the Home Office's assertion that the draft Bill does not extend criteria from what is required under existing legislation.
62. It is also important to understand the effect this broad extension will have on small and medium sized enterprises (SMEs), who may be unaware of new requirements that may affect them and the implications of these new requirements.

63. This is particularly important for small cloud service providers, who may be required to retain data to a period of time when they may not otherwise still have the data under normal business practices. For example, a data retention notice may impose an obligation on a small provider to retain data after the data controller, i.e. the customer in some cases, has deleted the data. This will make the provider the de-facto data controller and create a host of further obligations for the provider as the controller of the data. This stance may differ from the normal mode of operation of cloud service providers, where responsibility for the data is shared between the hosting provider and customer, and is an example of the draft Bill again altering the risk posture of UK businesses for the worse.

64. The original intention of bringing together various pieces of surveillance legislation into one Bill is to provide clarity and transparency to industry, agencies and the public. However, over-broad definitions such as these are counter to this goal.

The draft Bill must have proper oversight and authorisation

65. When introducing the draft Bill to Parliament on November 4th, the Home Secretary referred to an apparent "double-lock" authorisation regime for warrants that would strengthen the oversight and authorisation for certain investigatory powers.

66. The draft Bill puts forward a proposal to create an independent Investigatory Powers Commissioner (IPC) – a senior judge responsible for approving the authorisation of interception, bulk collection and equipment interference warrants (unless in urgent cases) and overseeing how the investigatory powers afforded to the security services are used.

67. One of the main shortcomings of current surveillance practices is that the oversight arrangements in place do not provide the involvement of an authority separate from the investigative apparatus, authorising, approving and reviewing warrants. David Anderson QC, the Independent Reviewer of Terrorism Legislation, earlier this year argued that the involvement of a judge in the authorisation process for interception warrants would bring the UK closer to other democratic nations and was an important step in facilitating international co-operation between like-minded, democratic countries.

68. It should however be noted that under Clause 19(2) the Judicial Commissioner, when reviewing a warrant, "must apply the same principles as would be applied by a court on an application for judicial review". The IPC is therefore limited in its role and will only be able to "approve" interception, bulk collection and equipment interference warrants and will not be responsible for authorising such warrants. This falls short of the recommendation by Anderson and is far from the "double-lock" that the Home Secretary claimed it to be.

69. According to the draft IP Bill, a Judicial Commissioner must review the "process" of the warrant being issued and base their approval on whether the warrant is "necessary" and "proportionate to what is sought to be achieved". This indicates that the role of the Judicial Commissioner is more procedural than authoritative and raises important questions as to the grounds as to which a Judicial Commissioner can refuse to approve an interception warrant.

70. As techUK has consistently called for in the past, in line with Anderson's recommendations, the IPC needs to be able to fully assess the substance of a warrant and be in a position to decide whether less obtrusive means are available by which the data in question could be obtained.

71. We recommend that the Joint Committee sufficiently investigate what the term "judicial review" means in practice and what the full role, responsibilities and functions of a Judicial Commissioner are. Will, for example, a Judicial Commissioner merely be involved in seeing whether proportionality has been assessed by Secretary of State or will they be able to assess the full merits of the warrant (including its necessity and proportionality) and not the process?

The draft Bill should not prohibit companies from disclosing the existence of a data request

72. Under the draft Bill, service providers will be able to appeal obligations (including Data Retention Notices) directly to the Secretary of State, who will be obliged to take advice from the Technical Advisory Board (TAB) and the Investigatory Powers Commissioner. The circumstances in which appeals will be permitted will be broadened to take account of changes to a company's services and infrastructure.

73. Although the draft Bill correctly allows companies to appeal warrants directly to the Secretary of State, it is concerning that Section 77(2) prohibits companies from disclosing the existence and contents of a data retention notice.

74. Transparency is crucial to ensuring that confidence in surveillance practices going forward is maintained – for this reason, more and more companies are now producing transparency reports on the number and nature of requests that they receive for data. Section 77(2) prohibits some companies from having the same opportunity and also prevents companies from communicating with each other about a notice (should they wish to do so) and share technical solutions to retention notices. The Committee may wish to consider whether this provision helps the draft

Bill achieve its stated objective of greater transparency and openness regarding government requests for data.

The Technical Advisory Board should include the breadth of the technology industry and legal experts

75. Furthermore, the Technical Advisory Board that the Secretary of State is obliged to take advice from should be drawn from a wider pool of telecommunications operators, such as cloud service providers, given the broader scope of the legislation and the fact that it will potentially apply to a broader range of companies. This will ensure that the breadth of the industry has a voice on the TAB, that it has the right technical and legal competencies and that it is clearly independent as a place where companies would go to seek appeals. The TAB should also have expertise on cost and legal matters, as it will have an extraordinarily important role to play in what is going to be a fast moving and dynamic area.

Conclusion

76. Surveillance legislation to date has not worked in the public interest and has been unnecessarily vague. User expectations of transparency have increased since 2010 and, if implemented correctly, the draft Bill can take a global lead in introducing strong oversight powers and a clear international framework for the lawful acquisition of data from overseas on the other.

77. techUK welcomes the process that has been undertaken around the Investigatory Powers Bill to date. We understand that the Joint Committee has limited time to scrutinise what is an important, but complex, legislation and is willing to support its work in order to ensure that the UK gets legislation that will balance consumers' desire for privacy and security with industry's legal requirements to support the security services in their vital work.

78. techUK's written evidence has highlighted some key areas that the Joint Committee must consider when scrutinising the draft Bill – in particular, issues related to the necessity and proportionality of many of the provisions within the draft Bill; the clarity that the draft Bill gives to the technology sector; and the future potential use and implications of the powers proposed.

79. The evolution of the technology sector, and its future growth, mean that the Joint Committee must also consider the future use of the draft Bill and whether its provisions will stand the test of necessity and proportionality as technology changes. techUK has been a willing partner in discussions to date and is keen to remain an informative voice in the future as the draft Bill is put before Parliament.

21 December 2015

Alice Thompson—written evidence (IPB0072)

My name is Alice Thompson I am writing to you on behalf of the Thompson family

I have been using the internet for a long time

I am sad and disappointed that we have to go through with the draft investigatory powers bill

I agree that we have a right to security but I also agree that the security and police service's need to respect the right to privacy and not to spy on innocent people who have not committed any crime

There are thing in this bill that I can't agree with

The powers are overreaching

This bill will endanger privacy by allowing the security services to spy on everyone

Internet connection records
Why collect records about every internet website I been on and every app I have used ?
It's an invasion of privacy and it would be costly to run

Encryption
I have been using encryption to pay my mum and dad using Halifax a banking website I have also used encryption for shopping on the internet I have also used encryption to talk to my mum and dad and to communicate using WhatsApp twitter skype it would be very sad if apple left the UK because the government banned encryption

Please could these powers be taken out of the bill?

21 December 2015

HH Judge Peter Thornton QC—written evidence (IPB0026)

PROPOSAL FOR EXTENSION OF MEANING OF 'RELEVANT JUDGE'

1. The Chief Coroner proposes that the meaning of "a relevant judge" in paragraph 21, Schedule 3 to the Investigatory Powers Bill (IPB), be extended for the benefit of certain coroner investigations. Under section 6 of the Coroners and Justice Act 2009, an investigation by a coroner includes an inquest in most cases.

2. Paragraph 21, Schedule 3 to IPB replicates section 18(11) of the Regulation of Investigatory Powers Act 2000 (RIPA). It provides, as an exception to matters that may be excluded from legal proceedings, that disclosure of certain material may be made to "a relevant judge" in a case in which that judge has ordered the disclosure to be made to him/her alone.

3. There is therefore no change to the list of relevant judges who may view RIPA material in legal proceedings (which has been held to include inquests: see Hallett LJ in *7/7 Inquests,* Ruling 3 November 2010). This list excludes three categories of persons who may conduct coroner investigations (and inquests) under the Coroners and Justice Act 2009: retired High Court and Circuit judges, all coroners and former senior coroners under the age of 75.

4. The Chief Coroner's proposal is that certain retired judges and a limited number of senior coroners should become relevant judges for IPB purposes.

5. The Lord Chief Justice, at the request of the Chief Coroner, may nominate a person to conduct an investigation (and inquest) into a person's death: paragraph 3(1), Schedule 10 to the Coroners and Justice Act 2009. Such persons include a judge of the High Court, a Circuit judge or a person who held office as a judge of the Court of Appeal or of the High Court (but no longer does so) and is under the age of 75: paragraph 3(2).

6. If a retired judge is nominated to conduct an investigation (including an inquest), he/she is prohibited from viewing RIPA/IPB material. Without being able to do so, the investigation and inquest process may be incomplete.

7. Similarly, a judge who is nominated in the same way before retirement to conduct an investigation (including inquest) which continues after the judge's retirement age may also be prohibited from viewing RIPA/IPB material.

8. The Chief Coroner therefore proposes that the list of persons who are "a relevant judge" in paragraph 21 of Schedule 3 to the Bill be extended to include: retired judges of the High Court or retired Circuit judges who are under the age of 75.

9. In addition the Chief Coroner proposes that the list in paragraph 21 of Schedule 3 should also include a cadre of six senior coroners of England and Wales, selected by the Chief Coroner and approved by the Lord Chief Justice, who are under the age of 75. This cadre is necessary because more and more coroner investigations (including inquests) involve intelligence material. Where this arises, and it would not be necessary for a judge to be

nominated to conduct the investigation (including inquest), the Chief Coroner could direct a senior coroner from the cadre to conduct the investigation (and inquest). The Chief Coroner could also arrange special training for the cadre of senior coroners.

HH JUDGE PETER THORNTON QC
CHIEF CORONER

16 December 2015

The Tor Project—written evidence (IPB0122)

Introduction

Background to The Tor Project and the Tor software

1 The Tor Project is a 501(c)(3) non-profit based in the United States, but with employees, contractors, and volunteers worldwide (including the United Kingdom). The Tor Project conducts research, training, and software development to improve Internet privacy and safety, and to promote human rights, free speech, free expression and civic engagement.

2 The Tor Project is predominantly funded by Non-Governmental Organisations (NGOs) and governments, as well as individual and corporate donations. Recent funders include the Swedish International Development Agency (Sweden), the Broadcasting Board of Governors (US), the National Science Foundation (US), the NLnet Foundation (Netherlands) and the Ford Foundation (US).

3 The core software product developed by The Tor Project, "Tor" was originally designed and implemented as a research project by the United States Naval Research Laboratory. The Tor software improves its users' safety while using the Internet by redirecting communications via the Tor network – approximately 7,000 computers ("nodes") operated by volunteers worldwide. The nodes chosen for a particular communication are selected randomly by the Tor software running on the user's computer.

4 Communications sent via Tor typically will pass through three nodes before being sent to the ultimate destination. Each of these Tor nodes will know the source immediately before it, and will know the next destination for the communication, but any one node will not know both the original source and ultimate destination for the communication. Communication between nodes, and between the user's computer and the Tor network are encrypted to protect against eavesdropping and tampering.

5 Through this approach, Tor protects users against someone observing their computer's Internet connection from discovering which websites they are accessing, and with whom they are communicating. This could be of importance, for example, to a journalist collecting information about human rights abuses from sources whose personal safety could be put at risk if the government discovered they were talking to journalists.

6 Tor also prevents websites from discovering the identity of visitors. This could be of importance, for example, to a law enforcement agency collecting intelligence from a website suspected to be involved in criminal activity. Equally, normal Internet users may desire privacy and want to protect their identity from websites who they are concerned might profile their behaviour and use it inappropriately or sell it.

7 A rapidly growing use of Tor is to allow users to circumvent national censorship schemes. Such censorship may be long term, such as the "Great Firewall of China", or can be responsive to events, such as the blocking of Facebook and YouTube by the Tunisian regime in the run-up to the late 2010/early 2011 revolution.

8 Other uses of Tor include victims of crime talking to fellow survivors anonymously, children protecting their personally identifiable information while using the Internet,

military personnel working undercover, operators of anonymous tip-lines reducing the risk of their sources being compromised, whistleblowers reporting on corruption, and financial institutions conducting due-diligence.

9 Further information about The Tor Project can be found on our website: https://www.torproject.org/

Use of the Internet by Human Rights Activists

10 This submission is not only based on how the Draft Investigatory Powers Bill would affect The Tor Project and users of its software, but also how the draft bill would affect more general use of the Internet by human rights activists. Information included in this submission is based on experience by Tor Project members in training human rights activists on how to effectively and safely use computers and the Internet.

11 Internet usage by Human Rights Activists can be broadly split into two categories.

12 Firstly there is the use of general-purpose Internet services, such as Facebook, YouTube, Twitter, Flickr, and webmail providers. These are popular amongst human rights activists for organizing their supporters because they are familiar, easy to use, and capable of withstanding bursts in demand that might swamp smaller services. They are also widely used outside of human-rights circles and so may draw less attention by the regime being defended against, and make it easier to get information out of the country to promote their case abroad.

13 Secondly, there are special-purpose tools designed with human rights activists as a significant (although perhaps not exclusive) target user group. Tools in this category include Tor and Martus (a software package developed by Benetech[1343] for securely collecting data of human rights abuses). Such tools are developed because there is a lack of security or functionality in general-purpose Internet services and software packages.

14 Both categories of usage are important, although performing a quantitative comparison is difficult. Use of general-purpose Internet services for human rights is likely to be more predominant, but while uses of special-purpose Internet services may be fewer in number they may be greater in their importance.

Comments on the Draft Investigatory Powers Bill

Security of stored communications and communications data

Addressing questions on secure retention of intercepted material, and requirements placed on service providers

15 The draft bill states that communications and communications data that is collected or processed as a result of powers granted by the bill should be protected from unauthorised access. Examples of such requirements include Clause 53, covering filtering arrangements, and Clause 74 covering retained communications data. However, evidence shows that the current state of the art in computer security is not sufficient to adequately protect communications or communications data, or to restrict access to facilities built to collect or process this material. Although there are techniques to protect computer systems from large-scale attacks, there are no effective measures for

[1343] https://www.martus.org/

protecting computer systems from targeted attack by a capable adversary, especially when an adversary with state backing is a possible threat (as is the case with communications and communications data concerning human rights activists).

16 This can be seen from the numerous breaches of security of communications service providers, even those who by far exceed industry standard levels of protection. It is likely that there are other cases of breaches that have not been disclosed due to commercial sensitivity.

17 One such example is the breach of Google's webmail service in December 2009[1344]. This attack was specifically targeted against Chinese human rights activists. The breach of Google was part of a co-ordinated and sophisticated attack that also included Adobe and other companies that chose not to be publicly disclosed[1345]. The attack made use of custom-made malware that was designed to, and succeeded at, avoiding detection by anti-virus software. It also exploited a vulnerability in Microsoft Internet Explorer which was, at the time of the attack, not known publicly. The identity of the attackers remains unknown and was disguised by transmitting their communications through hijacked computers in the US and Taiwan.

18 Another notable incident is the compromise of the Vodafone telephone exchange in Greece[1346], allowing attackers to bug the mobile telephone of over 100 high-ranking dignitaries, including the prime minister of Greece. In a highly sophisticated attack, custom-designed software activated the lawful-intercept functionality of the telephone exchange even though Vodafone had not purchased it. The attackers also successfully circumvented the audit logging, thereby hiding their unauthorised access. Eventually, the tampering was discovered, but only after almost a year of being active (the exact date the attack was perpetrated remains unknown).

19 As a final example, a hacker supportive of the Iranian government but who stated that he was not affiliated to the government, compromised the certification authorities DigitNotar and Comodo (and claims to have compromised others), and obtained digital certificates which were used to impersonate Google's website, potentially collecting sensitive information such as passwords, communications data, and content[1347]. The same attacker also targeted The Tor Project website, so it is reasonable to suspect that human rights activists were among the targets.

Sensitivity of Communications Data

20 The draft bill requests that communications data, not content, may be collected through a retention notice. The Home Secretary argued that communications data is less sensitive than content ("the modern equivalent of an itemised phone bill"), and thus does not deserve the same safeguards, restrictions on collection, or level of authorisation to access.

21 However, in many cases communications data can be as sensitive as content, and in some cases may be more sensitive than content.

[1344] http://googleblog.blogspot.co.uk/2010/01/new-approach-to-china.html
[1345] http://www.wired.com/threatlevel/2010/01/operation-aurora/
[1346] http://spectrum.ieee.org/telecom/security/the-athens-affair/
[1347] http://arstechnica.com/security/2011/09/comodo-hacker-i-hacked-diginotar-too-other-cas-breached/

22 For example, Internet Connection Records revealing that someone accessed a website which is collecting evidence on human rights violations could put that person or their family in severe danger. Internet Connection Records would also reveal whether someone had visited a site for people with cancer or alcoholism.

23 Even disclosing that someone was using the Internet at a particular time can be sensitive when it is correlated with, for example, the posting of videos of human rights abuses on YouTube. While the timing of a single instance of a video is unlikely to uniquely identify a person, repeating this exercise, with knowledge of the "usual suspects" for such activity, could single out an individual for repercussions.

24 Experiments have shown that 23.3% of Wikipedia users could be uniquely identified from Internet Connection Records alone, had they been using Tor to protect their privacy[1348]. This proportion goes to 95.7% when only Wikipedia users who have posted 50 or more items on Wikipedia are considered.

25 As another example, communications data showing that a phone call made by a journalist from a particular location could put that journalist at risk. It has been reported that the Syrian government was using Internet communications data analysis to target journalists. This technique has been implicated in the death of Sunday Times war correspondent Marie Colvin[1349].

26 Even “entity data”, while typically less sensitive than Internet connection records, can be of critical importance. The disclosure of the identity of a person pseudonymously blogging about sexuality, political or religious beliefs could put someone's employment at risk, even within liberal democracies.

27 The reason that communications data can be more sensitive than content is that it is more amenable to automated analysis, particularly when collected in bulk (as proposed by the draft bill). Content is designed for humans to read, and it is a challenging problem for computers to accurately interpret content. In contrast, communications data is designed for computers to interpret and so is far easier for computers to analyse. Communications data allows a more accurate and detailed profile of individuals to be built than is possible with current technology to interpret content.

28 The examples above show that the discussion of the draft bill should not centre on the false tradeoff between civil liberty and security. While it is undoubtedly not the intention of the Home Office, this draft bill will significantly harm the safety of human rights activists. The discussion of the draft bill thus can be framed as a tradeoff between giving additional powers to law enforcement in exchange for taking away the ability of human rights activists and human rights organisations to protect themselves.

29 In making this tradeoff it is also important to note that while a single breach of security is sufficient to compromise the safety of a human rights activist, the inability of law enforcement to obtain communications data relevant to a crime does not mean that the investigation will not succeed. There are frequently alternative sources of information that will result in a successful outcome of the case.

Safeguards

[1348] http://www-users.cs.umn.edu/~hopper/surf_and_serve.pdf

[1349] http://www.telegraph.co.uk/news/worldnews/middleeast/syria/9098511/Marie-Colvin-Britain-summons-Syria-ambassador-over-killing.html

Addressing safeguards on accessing communications, communications data and undertaking equipment interference activities

30 The draft bill proposes safeguards for access to communications and communications data, such as requiring approval by a senior officer before an application can be made, and requiring that service providers retain data securely.

31 As discussed above, it is unlikely that mechanisms to prevent unauthorised access to data, or interception facilities, will work as needed. Audit mechanisms, to detect authorised access, are for the same reasons likely to be possible to bypass.

32 Furthermore, law enforcement agencies and intelligence agencies will likely require that the queries processed under filtering arrangements (Section 51 of the draft bill) be themselves confidential (as the compromise of this data could interfere with investigations). Therefore it will likely not be possible for the service provider to properly audit access, and it will be challenging to safely store logs for any subsequent audit by the Investigatory Powers Commissioner.

33 Even ignoring the significant possibility of unauthorised access to stored communications or communications data, and ignoring the significant possibility of unauthorised enabling of interception functionality, the mere possibility that the powers in this draft bill will be exercised introduces harm.

34 This is because the cost and risk of adding new functionality to a computer system grows dramatically the later in the development process that the change is introduced. While it may be comparatively cheap to add new functionality while a system is on the drawing board, it will be much more expensive to add the same functionality once the system is deployed in the field.

35 Therefore, the fact that the powers in the draft bill might be exercised will lead to service providers and their equipment suppliers to put in place functionality to intercept and store communications data, even before any powers are exercised. Providers may adopt designs for their systems which facilitate interception, such as through greater centralisation, but which leave the systems more.

36 As a consequence, the risk of interception capability being activated without authorisation will increase. Furthermore, the same equipment will likely be sold to other countries which may use the same interception capability to spy on human rights activists.

37 It is also likely that other countries will use the fact that the UK is proposing such legislation as a justification for their own surveillance proposals. This pattern was recently seen when the Chinese state news agency capitalised on the Prime Minister's statement to the House of Commons contemplating the censorship of social networks during the 2011 riots[1350].

Responses from industry

[1350] http://opennet.net/blog/2011/08/amidst-riots-uk-calls-censor-social-media

38 The response of service providers to the risks to human rights activists that the proposed bill presents will depend on how important human rights activists, and others who depend in Internet security for their safety, are to the company's priorities.

39 For general-purpose Internet services, human rights activists are a relatively small proportion of their usage base, and while some providers have been proactive in protecting human rights activists from attack (such as Google[1351]), other commercial considerations will likely take priority, and these are better left stated by the companies themselves.

40 In contrast, Internet services designed for human rights activists will likely take a more proactive response in protecting users from harm and so are more likely to avoid being put in the position of having to compromise user safety by avoiding having a UK presence.

41 In the particular example of Tor, recall that it is the user's computer that chooses the path through the network, so if there is sufficient fear that UK nodes are unsafe, users are free to avoid UK nodes without any intervention of The Tor Project.

42 Projects, such as Tor, may also consider that carrying out software development in the UK is too high a risk, because the draft bill may allow developers to be compelled to assist in the implementation of an equipment interference warrant (Clause 101).

43 The creation of vulnerabilities in software through targeted equipment interference warrants or technical capability notices (Clause 189) not only puts the users of the system at risk, but also the developers because it creates the possibility that someone could intimidate the service provider staff into disclosing communications, private information or equipment data.

Circumvention

Addressing necessity of requirements

44 As can be seen with the attacks on Vodafone in Greece, Google and Adobe in the UK, and DigiNotar in Denmark (in all of these the identity of the attackers is unknown), it is well within the capabilities of sophisticated attackers to hide their traces by hijacking computers and using these as stepping stones. Hijacked computers are effectively being used as a telecommunications service provider, but will not fall under the control of this law because the owner of the hijacked computer will not know that it is being used as a telecommunications service provider.

45 There are well-known techniques[1352], and software available, for defeating tracing communications based on communications data. Specifically, messages are delayed, and extra "dummy" messages are added, at each point that communications are relayed. Such techniques incur a high overhead but an attacker who has hijacked a computer to act as a stepping stones will not be paying for the network resources and therefore will have no need to be concerned at the cost.

21 December 2015

[1351] http://www.guardian.co.uk/technology/2012/jun/06/google-state-sponsored-hacking
[1352] http://mixminion.net/

Trading Standards North West, Intellectual Property Group—written evidence (IPB0092)

RESPONSE SUMMARY

1. This response has been compiled by Trading Standards North West, Intellectual Property Group, representing 22 Local Authorities in the North West of England. Operational officers have contributed to the report ensuring it provides a viewpoint as to the needs of investigative officers with reference to the needs of the Service today.
2. The Trading Standards Service is essentially a law enforcement agency that sits within Local Authorities and whilst the role of Trading Standards is varied it is important to recognise those trading standards officers involved in criminal investigations very often deal with organised crime and criminality which crosses over into the same remit as the Police, e.g. class A drugs, weapons, etc.
3. Therefore, for the purpose of this response we have related the comments to Trading Standards, distinct from Local Authorities, in an attempt to distance the points raised from Local Authority departments that have been targeted as part of the media frenzy for what is regarded as the 'snoopers charter'.

4. Our response provides the following points for consideration:

    a. Trading Standards have a duty to enforce specific legislation, e.g. Trade Marks Act 1994, in order to do this the Service requires access to communications data (entity/events and some elements of ICRs – primarily in relation to the access of IP addresses). This is an urgent requirement given Counsel's Opinion *(see appendix 1)* in March 2015, see *Closing Comments*. We feel some of the definitions within the Bill require further clarification.

    b. Is the requirement for judicial approval for Trading Standards authorisations necessary, in line with the recommendations by David Anderson QC, IATL. Utilising NAFN as the SPoC for Trading Standards and maintaining the criminality threshold of 6 month custodial sentences, could provide a more robust and streamlined process for Trading Standards.

    c. The new legislative framework could consider injunctive and criminal sanctions for those telecommunications operators who choose not to assist law enforcement requests.

    d. Central Government could also work with international governments and internet organisations to achieve common protocols to facilitate the dissemination of data in relation to businesses/individuals trading on the internet. With the emphasis on preventing anonymity for those involved in criminality.

5. Finally, the majority of the criminal investigations referred to throughout this response relate to a number of national objectives:
    a. Consumers: they protect consumers from harm and protect the wellbeing of the country.

b. Intellectual Property Crime: continues to be a top four priority for the UK Government, as per the IP Crime Report 2014, "the National Crime Agency recognises the threat IP Crime poses to UK economic growth and maintains it as a priority for its new Economic Crime Command.
c. Small/medium sized businesses: have been identified as an opportunity to provide economic growth – the very businesses that are generally only protected and supported by Trading Standards – as recognised by the European Commission http://ec.europa.eu/enterprise/policies/sme/index_en.htm?cookies=disabled.

Overarching/thematic questions:

- Are the powers sought **necessary**?
  - Has the case been made, both for the new powers and for the restated and clarified existing powers?

6. It is our opinion as detailed in this response that Trading Standards powers are not adequate and that the Bill doesn't meet the requirements for the Service to deliver its current legislative duties as bestowed on it by the legislature.

- Are the powers sought **legal**?
  - Are the powers compatible with the Human Rights Act and the ECHR?
    No comment put forward.

  - Is the requirement that they be exercised only when necessary and proportionate fully addressed?
    No comment put forward.

  - Are they sufficiently clear and accessible on the face of the draft Bill? Is the legal framework such that CSPs (especially those based abroad) will be persuaded to comply?

7. In relation to murder, terrorism, paedophile and cases which involve an immediate threat to human life we believe the majority of CSP's will comply and assist law enforcement agencies in the UK. Although the speed at which the processes operate could be improved. However, in relation to lower level criminality we do not believe CSP's will be persuaded to comply without the means for law enforcement agencies to adopt some form of injunctive relief and/or criminal sanctions.

  - Are concerns around accessing journalists', legally privileged and MPs' communications sufficiently addressed?
    No comment put forward.

- Are the powers sought workable and carefully defined?

8. For the reasons put forward in this response, in relation to the specific wording of the Bill and to the Factsheet guidance provided, we believe clearer definition on the powers available for Trading Standards/Local Authorities are required, see below Definitions.

- Are the technological definitions accurate and meaningful (e.g. content vs communications data, internet connection records etc.)? Does the draft Bill adequately explain the types of activity that could be undertaken under these powers? Is the wording of the powers sustainable in the light of rapidly evolving technologies and user behaviours? Overall is the Bill future-proofed as it stands?

- Are the powers sought sufficiently **supervised**?
  - Is the authorisation process appropriate? Will the oversight bodies be able adequately to scrutinise their operation? What ability will Parliament and the public have to check and raise concerns about the use of these powers?

Judicial Approval

9. We feel the introduction of judicial approval for Trading Standards/Local Authority requests for RIPA (Regulation of Investigatory Powers Act 2000) in November 2012, was an opportunity for the Government to appease the ground swell of negative media, which in many cases emanated from one or two national tabloids, directed at the so called snoopers charter.

10. As such we fully agree with recommendation 66 put forward by QC David Anderson, Question of Truth:

> 66. The requirement in RIPA 2000 ss23A-B of judicial approval by a magistrate or sheriff for local authority requests for communications data should be abandoned. Approvals should be granted, after consultation with NAFN, by a DP of appropriate seniority within the requesting public authority.

and furthermore, with his comments in 14.82:

> 14.82. Recommendation 66 would reverse the recently-imposed requirement on local authorities to seek ***judicial approval by a magistrate or sheriff*** for communications data requests. Whilst judicial approval at this level may sound like a safeguard, and was no doubt required for that reason, the reality appears to have been that it has added time, complexity and cost to the authorisation process without contributing additional rigour to it: 9.98-9.100 above. Indeed it is very likely that the introduction of this requirement has resulted in applications being made less often than they should: 9.100.
>
> 14.83. I considered recommending extra training for magistrates, or centralising the judicial mechanism in the court centres closest to NAFN's Tameside and Brighton offices:[64] an option that has been rejected in the past. But despite the fact that the requirement for authorisation by magistrate or sheriff was only recently introduced, I have no hesitation in advising its removal. The independent SPoCs of NAFN perform a good service (9.95 above) and – subject to careful audit by the Commissioners, and in conjunction with local authority DPs – should provide the requisite protection against the improper use of local authority powers to authorise the acquisition of communications data.

11. The operational officers who have provided input to this response feel the scrutiny intended by the move to judicial approval in 2012 would be better provided by NAFN, in many cases the ability of the clerk to provide advice to the Magistrates is the determining factor. As far as we can see the judicial process was implemented with

minimal or no training given to Magistrates, whereas the SPoCs of NAFN are well trained and experienced to deal with these matters expeditiously.

12. We also agree with QC David Anderson's comments in relation to the process resulting in a reduction of applications, primarily due to the additional time and resource required to process and applies to the Magistrates, again at a time when officer numbers have been cut by 50%.

13. Furthermore, we feel the burden placed on officers in order to obtain judicial approval is likely to increase if proposals to restructure the Courts Service are implemented, as this will reduce the number of local Magistrates Courts. The impact of this will be officers will have to travel further to attend court, placing further time constraints on officer time, the downside of course being a further reduction in applications and less criminals brought to justice. As opposed to a smoother streamlined online electronic service which could be provided by NAFN.

Specific questions:

General

- To what extent is it necessary for (a) the security and intelligence services and (b) law enforcement to have access to investigatory powers such as those contained in the Draft Investigatory Powers Bill?

14. This question has been covered in the Definitions section below.

- Are there any additional investigatory powers that security and intelligence services or law enforcement agencies should have which are not included in the draft Bill?

15. SNS accounts that operate under closed privacy settings are essentially enabling the users to trade their wares behind closed doors, as the inability of Trading Standards to identify the individual or to obtain evidence of counterfeit/illicit goods for sale being sold via the account/group, mean the individuals are untouchable. This is effectively a Silk Road for the masses and as the majority of these offences are investigated by Trading Standards, it means they go uninvestigated.

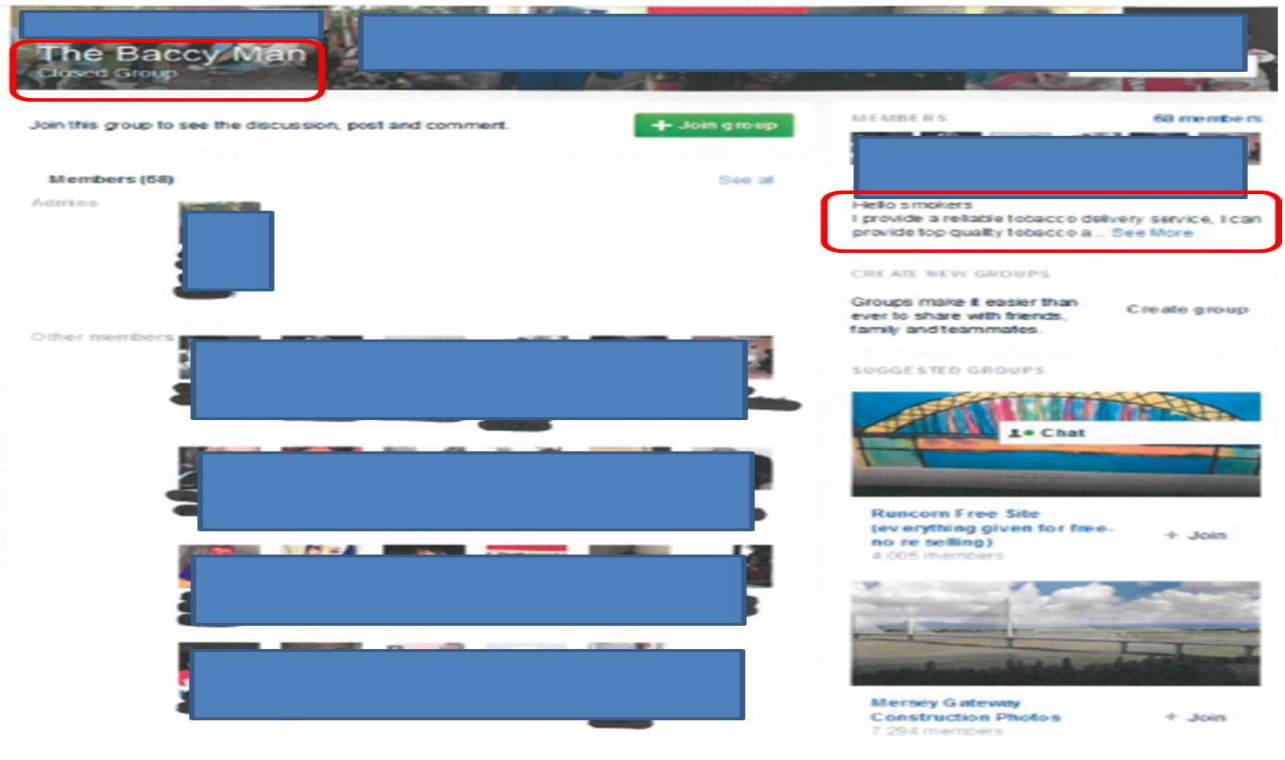
16. For example the following CAPP data, referred to below highlights the growth of Facebook connected complaints during the period 2010-2015:

    a. Since 2010/11 the number of complaints each year have consistently increased between 41-74%
    b. 6,566 Facebook complaints received during 2014/15 - an increase of 25% yr on yr, slightly down on the 41% increase the previous year
    c. Since 2010/11 the number of complaints have increased from 1,314 to 6566, representing an increase of 400% in five years

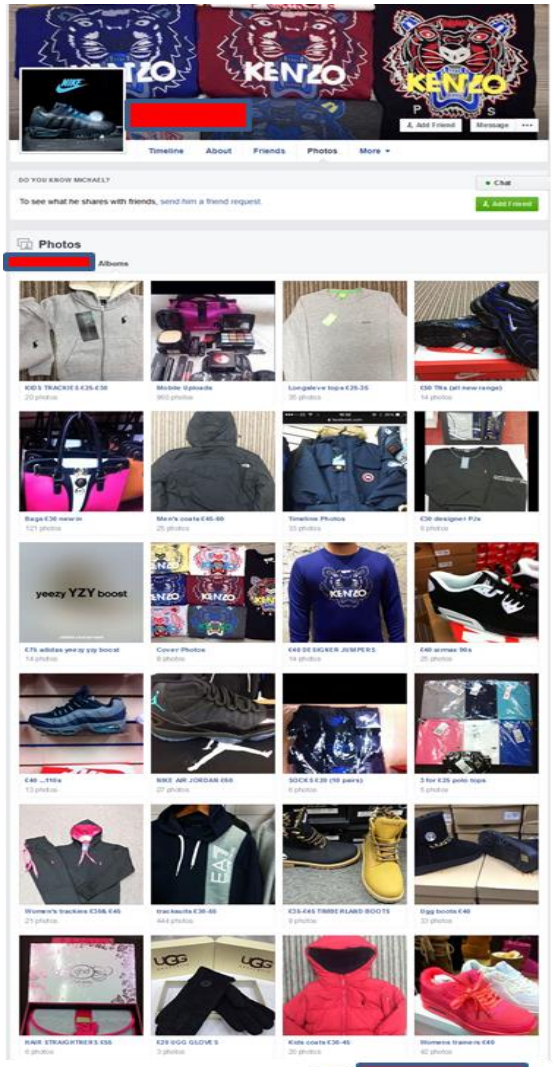
17. When considering the level of incidences relating to SNS/Facebook one should not forget the reported numbers may be considerably lower than other mediums involving criminality, this is because the majority of SNS/Facebook accounts consist of 'friends'

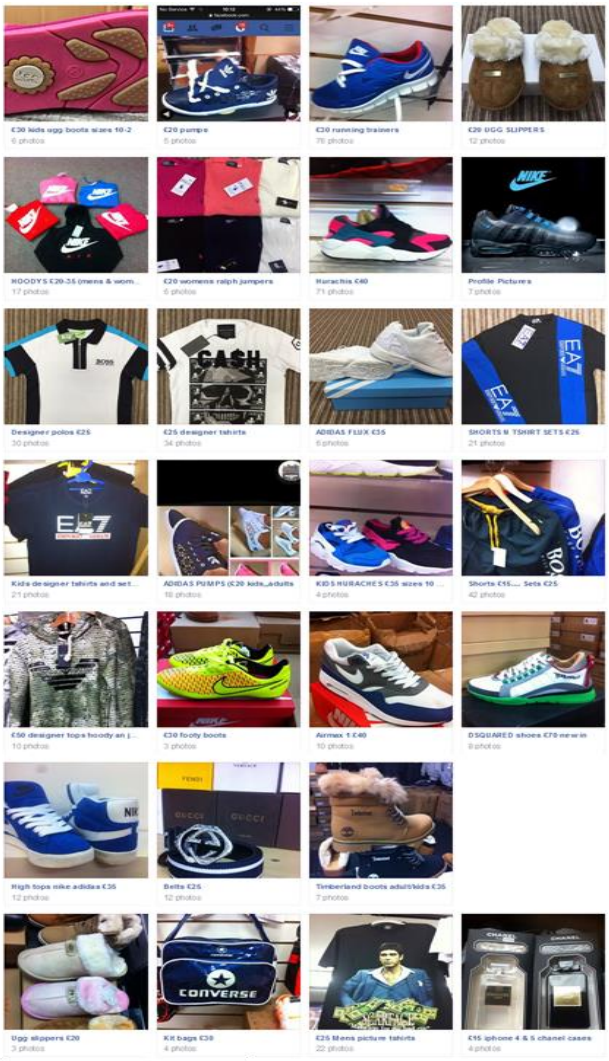
from a specific community or location and therefore, they are often reluctant to report criminality due to their relationships within the group and the associated fear factor of being identified as the informant.

18. Sample - Sanitised Criminal Accounts
    a. Closed Privacy Settings - Images and evidence of trade on these accounts aren't available for Trading Standards to view as they are categorised as content.



    b. Open Privacy Settings – these images are available, but without an IP address it isn't possible to identify the seller.





- Are the new offences proposed in the draft Bill necessary? Are the suggested punishments appropriate?

  No comment put forward.

Interception No comment put forward.

- Are there sufficient operational justifications for undertaking (a) targeted and (b) bulk interception?

- Are the proposed authorisation processes for such interception activities appropriate? Is the proposed process for authorising urgent warrants workable?

- Are the proposed safeguards sufficient for the secure retention of material obtained from interception?

- How well does the current process under Mutual Legal Assistance Treaties (MLATs) work for the acquisition of communications data? What will be the effect of the extra-territorial application of the provisions on communications data in the draft Bill?

Communications Data

- Are the definitions of content and communications data (including the distinction between 'entities' and 'events') sufficiently clear and practical for the purposes of accessing such data?

Definitions

19. We understand the Bill has been written with the wider security, law enforcement and anti-terrorism agencies in mind, however, we have concerns from a Trading Standards perspective as to some of the definitions and wording provided both in the Bill and in the Factsheets provided by the Government as part of the overall draft release of the Bill. Definitions of primary concern are those in relation to communications data, specifically 'internet connection records', 'events data' and 'entity data'.

20. The definitions within s.193 make reference to each element referred to above, except ICRs, namely:

Entity data

(3) "Entity data" means any data which—
  (a) is about—
    (i) an entity,
    (ii) an association between a telecommunications service and an entity, or
    (iii) an association between any part of a telecommunication system and an entity,
  (b) consists of, or includes, data which identifies or describes the entity (whether or not by reference to the entity's location), and
  (c) is not events data.

Other definitions

(7) "Entity" means a person or thing.

Events data

(4) "Events data" means any data which identifies or describes an event (whether or not by reference to its location) on, in or by means of a telecommunication system where the event consists of one or more entities engaging in a specific activity at a specific time.

21. The Factsheet (Bill Definitions) provides the following examples for entity (note reference to IP address) and event data (note reference to an ICR):

Examples of entity data	Examples of events data
Phone numbers or other identifiers linked to customer accounts; customer address provided to a communications service provider; IP address allocated to an individual by an internet access provider.	The fact that someone has sent or received an email, phone call, text or social media message; the location of a person when they made a mobile phone call or the Wi-Fi hotspot that their phone connected to; an internet connection record.

22. The definition for ICRs (note reference to 'a kind of communications data') can be found in the Guide to Powers & Safeguards accompanying the draft Bill, whereby they are defined as:

INTERNET CONNECTION RECORDS

What are they?

44. A kind of communications data, an ICR is a record of the internet services a specific device has connected to, such as a website or instant messaging application. It is captured by the company providing access to the internet. Where available, this data may be acquired from CSPs by law enforcement and the security and intelligence agencies.

45. An ICR is not a person's full internet browsing history. It is a record of the services that they have connected to, which can provide vital investigative leads. It would not reveal every web page that they visit or anything that they do on that web page.

23. The Guide also provides that, Local Authorities (Trading Standards) will be prohibited from acquiring ICR's, as does the Bill, s.123:

What safeguards will there be?

50. Applications to acquire ICRs can only be approved using the stringent application process for communications data requests (see paragraph 24-25 above) and only for a limited set of statutory purposes and subject to strict controls. Local authorities will be prohibited from acquiring ICRs.

123 Local authorities will be prohibited from acquiring internet connection records for any purpose.

24. Furthermore, s.47(6) provides a definition for ICRs:

(6) In this section "internet connection record" means data which—

(a) may be used to identify a telecommunications service to which a communication is transmitted through a telecommunication system for the purpose of obtaining access to, or running, a computer file or computer program, and

(b) is generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication (whether or not a person).

25. s.57(3) confirms local authorities can have access to communications data for the purposes of preventing and detecting crime as per s.46(1)(a) and s.46(7)(b):

Local authorities

57 Local authorities as relevant public authorities

(1) A local authority is a relevant public authority for the purposes of this Part.

(2) In this Part "designated senior officer", in relation to a local authority, means an individual who holds with the authority—

(a) the position of director, head of service or service manager (or equivalent), or

(b) a higher position.

(3) A designated senior officer of a local authority may grant an authorisation for obtaining communications data only if section 46(1)(a) is satisfied in relation to a purpose within section 46(7)(b).

(4) The Secretary of State may by regulations amend subsection (2).

(5) Sections 58 and 59 impose further restrictions in relation to the grant of authorisations by local authorities.

26. Similarly, the Factsheet – Bill Definitions confirms communications data to be:

Communications data

- Communications data is data held by a CSP or available directly from the network which identifies a person or device on the network, ensures that a communication reaches its intended destination, otherwise describes how communications move across the network or otherwise describes how a person has been using a service.
- It is categorised into:
  - *Entity data* – This data is about entities or links between them but does not include information about individual events. Entities could be individuals, groups and objects (such as mobile phones or other communications devices).
  - *Events data* – Events data identifies or describes events which consist of one or more entities engaging in an activity at a specific point, or points, in time.

27. ICR appears twice in the Factsheet – Bill Definitions and it appears to make reference to them being a higher level of communications data in the form of 'events data' as per the bullet point below and yet the example provided above refers to ICR as being an element of events data:

The authorisation levels required to access communications data reflect the fact that the set of events data as a whole contains the more intrusive communications data., including information on who has been in communication with whom, a person's location and internet connection records. Access to events data is authorised at a higher level within public authorities.

28. The Factsheet - ICRs confirms the following:

Why do we need it?

- Evidence indicates that the majority of criminal suspects are using online communications services, and other online services of potential investigative value, that are currently invisible to communications data requests. Ofcom statistics also show that the

- ICRs can be crucial for:
  - Identifying the sender of an online communication (often involving IP address resolution)

- It will involve retention of a destination IP address but can also include a service name (e.g. Facebook or Google) or a web address (e.g. www.facebook.com or www.google.com) along with a time/date.

This is precisely why Trading Standards require access to IP addresses.

29. The Bill definition of Communications Data can be found in s.193(5), which again makes no reference to ICRs:

Communications data

(5) "Communications data", in relation to a telecommunications operator, telecommunications service or telecommunication system, means entity data or events data—

(a) which is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator and—

(i) is about an entity to which a telecommunications service is provided and relates to the provision of the service,

(ii) is comprised in, included as part of, attached to or logically associated with a communication (whether by the sender or otherwise) for the purposes of a telecommunication system by means of which the communication is being or may be transmitted, or

(iii) does not fall within sub-paragraph (i) or (ii) but does relate to the use of a telecommunications service or a telecommunication system,

(b) which is available directly from a telecommunication system and falls within sub-paragraph (i), (ii) or (iii) of paragraph (a), or

(c) which—

(i) is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator,

(ii) is about the architecture of a telecommunication system, and

(iii) is not about a specific person,

but does not include the content of a communication.

30. For completeness paragraph 25 of the Guide, 'what safeguards there will be', which refers to the SPoC function provided by NAFN (generally utilised by Local Authorities/Trading Standards for SPoC approval) which confirms TS/LAs ability to access communications data.

> 25. Once it has gone through the SPoC, the authorisation will be signed off by a Designated Person (DP), who is independent of the investigation for which the communications data is needed. The draft Bill will provide a power that can ensure public authorities that access communications data infrequently will have to go through a shared SPoC (for example, by making use of the SPoC function within the National Anti-Fraud Network, as recommended by David Anderson QC). This will help to ensure that all applications are consistent and of sufficient quality.

31. In light of the definitions above it is our understanding that Trading Standards have access as per the following:

    a. **Entity Data** – this appears to be the information relating to the individual's account, essentially the basic subscriber information, name, address, bank account details, initial log on IP address, and any other information linked to the setting up of the account.

    b. **Events Data** – this appears to involve the processes of the communication by the entity, e.g. the sending/receipt of an email, or telephone calls made/received

32. Our interpretation of the above elements of the Bill in relation to potential trading standards investigative scenarios are as follows:

    a. email received by a complainant from a **fraudulent website operator** - officers wish to trace the sender via IP address resolution - this would be classed as event data and therefore accessible under communications data

    b. **social networking site** (SNS): an individual operating a SNS account involved in the sale of counterfeit GHD hair straighteners – officers would want the basic account information (often fictitious) and IP address, to identify the individual via IP address resolution
        - this would potentially be classed as entity data if the CSP has captured the information as part of the subscriber account set up, i.e. it is held in an account file
        - however, if the CSP has to process data to obtain the said IP address then the TS/LA wouldn't be able to access the data, as it would be classed as ICRs, see s.47(5):

> (5) A designated senior officer of a local authority may not grant an authorisation for the purpose of obtaining data which is already held by a telecommunications operator and which is, or can only be obtained by processing, an internet connection record.

- this creates a lottery for the investigative officer as the availability of the IP address will depend upon how the CSP stores the account data and whether or not they have to process an ICR

  The issue with both 1 & 2 is that it provides a lottery scenario for the investigative officer. If the CSP automatically collates and stores IP addresses in an account file, then it can be accessed by the TS/LA if however, if it has to 'process it' then it isn't accessible. The irony being that it is the same data just processed differently.

  Also, generally speaking the majority of internet users utilise 'dynamic' IP addresses which are allocated to the user as and when they access the internet. We are unsure as to whether or not a dynamic IP address would fall under event data or ICR classification, or is it purely down to how the data has been stored/accessed.

c. **internet site** offering scam holiday lets - whereby the officer wishes to identify the owner's details via IP address resolution via the hosting company.

   - we assume this would also fall under the classification of entity data as it relates to the individuals contact details held on the account

d. **VOIP** (voice over internet protocol), e.g. Skype, a complainant scammed by an escort agency which has communicated over VOIP – whereby the officer would need to identify the owner of the IP address to apprehend the criminal behind it.

   - we think this might fall under event data, although it could just as easily be classed as an ICR

e. **Mobile Phone Application**, e.g. WATS APP or a **Games Console**, e.g. xBox, used by two individuals who have been involved in the manufacture and supply of large quantities of counterfeit vodka - whereby the officer would be seeking the IP address of the recipient account holder.

   - similar to VOIP we would anticipate these data requests would fall under event data or an ICR

33. In response to the original question:

"Are the definitions of content and communications data (including the distinction between 'entities' and 'events') sufficiently clear and practical for the purposes of accessing such data."

we think the technical definitions covering the categories of data require substantial clarification in relation to exactly what data it is that Trading Standards will have access to. In all of the scenarios above we are unsure as to the ability of Trading Standards to

obtain access to the IP address and data that would enable the successful investigation of complaints and the associated criminality.

34. Therefore, we would strongly appeal for clarification of the definitions in relation to communications data, i.e. entity data, events data and ICRs, both in the wording of the Bill and in the supporting guidance/Factsheets provided. This is to ensure Trading Standards officers are aware of the parameters to which they have to work within and in the event the appropriate powers are not available, to prioritise their workload accordingly.

35. In not having access to IP addresses, whether entity or events data or classed as an ICR, many Trading Standards investigations will fail and the Service will not be able to comply with the duties imposed by Parliament. Ironically for the high volume/low level criminality examples we have referred to above, the Police will have access to the data required by Trading Standards officers, however, in the majority of cases they will not be investigated by the Local Policing Units. Therefore, this level of criminality will go uninvestigated, unpunished, consumers will continue to be ripped off by unscrupulous traders and criminals and complainants will not be recompensed.

36. As to whether the Bill is future proofed, for Trading Standards we do not feel it meets the present day requirements to enable officers to effectively carry out their duties. As 'no go areas' with regard to ecrime investigations already exist, e.g. SNS provide a prime example, there are thousands of Facebook users or groups who utilise the SNS platform to sell counterfeit & illicit goods such as tobacco, cigarettes, alcohol, cosmetics, electrical goods and clothing.

- Does the draft Bill allow the appropriate organisations, and people within those organisations, access to communications data?

  See Definitions section above.

- Are there sufficient operational justifications for accessing communications data in bulk?

  No comment put forward.

- Is the authorisation process for accessing communications data appropriate?

  See comments above regarding judicial approval.

Data Retention

- Do the proposed authorisation regime and safeguards for bulk data retention meet the requirements set out in the CJEU *Digital Rights Ireland* and the Court of Appeal *Davis* judgments?

No comment put forward.

- Is accessing Internet Connection Records essential for the purposes of IP resolution and identifying of persons of interest? Are there alternative mechanisms? Are the proposed safeguards on accessing Internet Connection Records data appropriate?

  See above response in Definitions.

- Are the requirements placed on service providers necessary and feasible?

  No comment put forward.

Equipment Interference No comment put forward.

- Should the security and intelligence services have access to powers to undertake (a) targeted and (b) bulk equipment interference? Should law enforcement also have access to such powers?

- Are the authorisation processes for such equipment interference activities appropriate?

- Are the safeguards for such activities sufficient?

Bulk Personal Data No comment put forward.

- Is the use of bulk personal datasets by the security and intelligence services appropriate? Are the safeguards sufficient for the retention and access of potentially highly sensitive data?

Oversight No comment put forward.

- What are the advantages and disadvantages of the proposed creation of a single Judicial Commission to oversee the use of investigatory powers?

- Would the proposed Judicial Commission have sufficient powers, resources and independence to perform its role satisfactorily?

- Are the appointment and accountability arrangements for Judicial Commissioners appropriate?

- Are the new arrangements for the Investigatory Powers Tribunal including the possibility of appeal adequate or are further changes necessary?

CLOSING COMMENTS

37. We are a professional Service, which has recently been awarded Chartered status to reflect that position. We enforce a wide range of legislation, with an array of offences and penalties, ranging from civil measures to indictable penalties up to ten years plus at the top end of the range. Whilst it is true that Trading Standards/Local Authorities

account for less than 1% of applications, we feel it is important that the Bill meets the needs of Trading Standards and provides the tools to deliver the duty to enforce, as has been bestowed on the Service by Government.

38. It is this duty to enforce which separates the Service from the role of the Police, for example s. 93, Trade Marks Act 1994: (1) It is the duty of every local weights and measures authority to enforce within their area the provisions of section 92 (unauthorised use of trade mark, &c. in relation to goods).

39. If the Service is truly to meet those duties then it should be given the necessary powers to fulfil them. Recent austerity cuts have hit hard across all Government departments, but for a Service cut by almost 50% in recent years it is essential that officers have the necessary tools to tackle issues effectively and efficiently. As such the Service needs the powers referred to, now more than ever, in order to fight crime, protect the public it serves, and to assist in driving local and national economies by supporting legitimate businesses.

40. Before austerity cuts took hold there was an appetite across Police forces to take on some of the crossover crimes referred to earlier, e.g. intellectual property crime, fuelled to an extent by the availability of monies from the proceeds of crime. However, since the cuts have taken hold the local Police forces have refocused their activities with a drive to provide community policing, which has seen the development of Local Policing Units and a return to good old fashioned policing strategies. In return that appetite for intellectual property crime has diminished and a depleted trading standards service is struggling to deliver its duties.

41. Ironically whilst the Bill provides the tools and powers for the Police to investigate crimes effectively and although the NCA (National Crime Agency), PIPCU (Police Intellectual Property Crime Unit), and the likes have the skills and resources to deal with ecrime investigations, Local Policing Units do not. Whilst local Police forces have CII's (Covert Internet Investigators) they deal with 'serious crime' and not high volume/low value crime.

42. The NTSECT (National Trading Standards eCrime Team) are subject to the same restrictions on access to data as local trading standards officers and whilst the team investigate trading standards offences on a national level they do not investigate local level criminality. Whereas, local trading standards services have trained specialist officers capable of conducting online investigations, but without the appropriate powers they are unable to carry out these type of investigations. This inability to investigate, which involves high volume/low value crime, means these type of crimes will go unresolved as there is no alternative enforcement agency to fill the void.

43. Historically, Trading Standards Enforcement Officers (TSO) have been given IP addresses by CSPs, that have been used to identify offenders. Although in light of Counsel's Opinion received in March 2015 this should not have been the case, Trading Standards has never been authorised to access IP addresses or content data.

44. Counsel's Opinion *(see Appendix 1)* in March 2015 provided an in depth review of Trading Standards powers and their capability to enforce legislation with a statutory duty to enforce, specifically in relation to SNS (Social Networking Sites). The results were damning, the Opinion confirmed that Trading Standards have no powers to obtain IP addresses from CSPs (Communications Service Providers), reducing their ability to investigate crime and to apprehend offenders. The Opinion focused upon SNS and the inability of Trading Standards Officers to investigate offences on SNS where privacy settings on the accounts were closed. Due to Trading Standards/Local Authorities not being authorised under the Regulation of Investigatory Powers Act 2000, to access communications/traffic data.

45. Finally, the Bill frequently refers to law enforcement we would seek clarification which agencies this term refers to and also whether Trading Standards falls under that classification.

APPENDIX 1

OPINION ON SOCIAL NETWORKING SITES:

SUMMARY

---

1. We are instructed by the Trading Standards Department of Halton Borough Council (supported by Trading Standards North West) and the National Trading Standards Board to provide an Opinion on various aspects of the investigation and prosecution by trading standards departments of cases involving social networking sites (referred to as 'SNS' and 'SNSs' accordingly). We have set out below a summary of some of the salient points, which are addressed in more detail in our full Opinion.

Background

2. SNSs are increasingly being utilised as a medium for all manner of cybercrime, including the sale of counterfeit goods, illegal and illicit goods, scams and other consumer protection offences.[1353] We can say that this reported trend is certainly becoming much more evident in cases in England and Wales in which we are professionally involved. Unlike user content published over public internet forums such as eBay, users of social media are increasingly able to use SNS privacy settings to control the audience for their content and communications. Some SNSs allow privacy or sharing settings to be adjusted so that content and communications are not visible to users outside of an authorised or selected group or

[1353] We have been provided with information including CAPP data on the increase in complaints relating to Facebook, including a more than 300% increase between 2010/11 and 2013/14

list; users can even 'micro manage' the audience for specific content or communications. These aspects of cybercrime on SNS platforms present a host of potential problems for TSOs investigating cases.

3. Trading standards departments in England and Wales may experience great difficulty in securing the co-operation or compliance of SNS providers with requests for basic information on user accounts and also requests to remove suspected criminal content. This problem is not uncommon to all UK law enforcement, particularly in relation to the investigation of less serious crime. Although, according to statistics published by the leading SNSs, compliance rates with requests from the UK are allegedly higher than elsewhere, we understand that obtaining disclosure of communications data from SNSs is still a significant problem. One of the most pressing problems facing a trading standards investigation is the apparent lack of power to deal with reluctance or outright refusal by an SNS provider to cooperate or comply with such requests for information. The problems are twofold:

(a) SNSs such as Facebook are typically based outside of the UK and may refuse to respond to requests for disclosure of communication data or dispute the application of the *Regulation of Investigatory Powers Act 2000* (as amended) ('RIPA'); and,

(b) SNSs process and retain data on servers located outside the UK, hence there is no data controller within the UK.

4. The position was succinctly summarised in relation to the Draft Communications Data Bill:

> 'RIPA is drafted so as to attempt to give United Kingdom public authorities a legal basis for requesting communications data from CSPs based overseas if they operate a service in the United Kingdom. However, many overseas CSPs refuse to acknowledge the extra-territorial application of RIPA. The procedure can of course be used to request access to data, and many CSPs will comply but emphasise that they are doing so on a voluntary basis; others will refuse to respond to RIPA requests at all. At that stage the only way in which United Kingdom law enforcement authorities can access the data is through the arrangements for international mutual legal assistance which allow the judicial and prosecuting authorities of one state to seek from the authorities of another state help in the prevention, detection and prosecution of crime…'[1354]

5. Historically, in the event of a refusal to comply with a request or a denial of jurisdiction, there have been difficulties with enforcement communications data requests under RIPA and other requests. Although we are generally aware from practice that this is a problem all UK law enforcement agencies might encounter to some degree or another, we understand this to be rather acute at the local authority level, particularly as some SNS

[1354] See: http://www.publications.parliament.uk/pa/jt201213/jtselect/jtdraftcomuni/79/7905.htm#a8

providers have historically refused to acknowledge the right of local authorities to obtain communications data.

6. RIPA provides a framework under which local authorities in England and Wales may be authorised to carry out a range of covert investigatory techniques. Whereas unlawful interception is specifically an offence under RIPA, although failure to otherwise carry out an investigation in accordance with RIPA is not an offence it runs the risk that in any proceedings evidence could be excluded under the Police and Criminal Evidence Act 1984 or the proceedings stayed as an abuse of process. In addition, a failure to obtain RIPA authorisation where Article 8 rights have been engaged could expose a local authority to a claim under section 6 of the Human Rights Act 1998.

7. There are three main investigatory 'tools' under RIPA that TSOs may consider using in an investigation involving an SNS:

(a) The use of 'directed surveillance' which is essentially covert surveillance carried out in places other than residential premises or private vehicles which is relevant where an investigatory technique might infringe Article 8 rights (e.g. where personal data or sensitive personal data is likely to be accessed or acquired and there is an expectation of privacy);

(b) The use of a covert human intelligence source (CHIS) which includes undercover officers (most significantly including covert profiles), informants and persons making test purchases; and,

(c) Powers to acquire or obtain 'communications data'. Communications data falls into three distinct types and since 2010 local authorities have only been to obtain the 'less intrusive' types of communications data (see below).

8. Importantly, the above powers cannot simply be used as a matter of course in any investigation involving an SNS. As the use of covert and intrusive powers under RIPA can potentially engage infringe an individual SNS user's Article 8 rights, the designated person in the local authority must be satisfied that the interference (including any collateral intrusion) is both necessary and proportionate. Assessment must be carried out on a case-by-case basis according to the particular facts of the case.

9. Since important amendments were made to RIPA in 2012, local authorities in England and Wales are subject to two further constraints—

(a) From 1 November 2012, local authorities in England and Wales authorising the use of directed surveillance, the acquisition of communications data or use of a CHIS under RIPA must obtain an order approving the grant (or renewal of an authorisation or notice) from a Justice of the Peace[1355] before

[1355] i.e. a District Judge or lay magistrate

it can take effect. Before a RIPA authorisation can be approved, the Justice of the Peace must also be satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate.

(b) Directed surveillance is subjected to a 'crime threshold' which essentially means that a local authority can now only authorise the use of directed surveillance where it is investigating particular types of criminal offences: criminal offences which attract a maximum sentence of six months' imprisonment or more and offences relating to the underage sale of alcohol or tobacco.

10. Our understanding is that trading standards investigations into cases involving criminality via social media are being hindered due to the following principal factors—

(a) even if an SNS does co-operate, local authorities have limited powers under RIPA, most importantly a lack of power to acquire traffic data, which often leads to practical difficulty in identifying a suspect and / or suspect's location;

(b) financial cuts in recent years have limited resources within local authorities and affecting the ability of trading standards to commit officers to investigations involving SNSs, particularly where RIPA techniques are or are likely to be engaged;

(c) the SNSs concerned are based outside the UK and the communications data sought in order to identify suspects is stored on one or more servers which are located overseas (possibly in multiple locations and possibly in more than one country);

(d) although local authorities may use the National Anti-Fraud Network to make requests under RIPA for communications data, local authorities lack enforcement powers against an overseas SNS;

(e) the enforcement provisions for injunctive relief in the event of non-compliance are within the remit of Secretary of State, which we think are unlikely to be invoked in the case of a typical trading standards investigation.

Problems in identifying suspects

11. The identification of an SNS user as a tangible subject of investigation may prove problematic for investigating officers, particularly in cases where privacy settings have been engaged by the SNS user. Where the identity and / or geographic location of an SNS user cannot be ascertained from content that is available on the SNS,[1356] RIPA provides a

[1356] E.g. descriptive information such as the name, geographical location etc. added by a SNS user's profile information; geolocation of individual posts and other information that can potentially be included in content added to the SNS by an SNS user

structure for designated public authorities to request and / or obtain what it describes as 'communications data' from postal and telecommunications service providers.

12. Local authorities are designated to make such requests and thus authorised to obtain (at least certain types of) communications data. RIPA divides communications data into three broad types:

(a) traffic data;

(b) service use information;

(c) subscriber information.

13. The principal difficulty a TSO is likely to encounter in investigating an SNS user whose name and / or location are unknown is the preclusion of local authorities using the RIPA provisions to obtain 'traffic data'. This is echoed by the Home Office guidance issued to local authorities, which expressly says: 'Under no circumstances can local authorities be authorised to obtain traffic data under RIPA'.[1357] Arguably, local authorities might obtain an IP address (classed as traffic data) from an SNS if the SNS has treated it as subscriber information within the meaning of RIPA (e.g. where an IP address has been recorded in the user account information by the SNS).[1358] However, in practice, the position is liable to be far more complicated: a communications service provider is likely to have to access traffic data to deal with a request for subscriber information containing an IP address.[1359] Although it seems this will not necessarily be problematic for those public authorities that are entitled to obtain all classes of communications data (i.e. both traffic data as well as subscriber information),[1360] local authorities are not permitted to request traffic data under section 21(4)(a) of RIPA and our view is that this would ultimately preclude obtaining and using IP addresses as part of the subscriber information.

14. Whether or not an SNS such as Facebook is subject to Part I, Chapter II of RIPA [1361] is debatable, as is the question of whether communications data held by an SNS comes within the meaning of "telecommunications data" or of "electronic communications data" or both. The position is somewhat clouded by the stance taken by providers such as Facebook, which have established disclosure policies to which both domestic and overseas law enforcement agencies are referred, yet will often reiterate that they will comply with requests for communications data on a voluntary basis.

[1357] See 'Protection of Freedoms Act 2012 – changes to provisions under the Regulation of Investigatory Powers Act 2000 (RIPA) Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance (Home Office, 2012)

[1358] see: the Home Office draft Code of Practice on Acquisition of Communications Data (Home Office, March 2015), which refers to static IP

[1359] To do this, a provider would typically have to access a history of dynamic IP addresses and check this against the account user. Dynamic IP addresses are unequivocally traffic data and communications data which local authorities in England and Wales are not entitled to obtain or use under RIPA.

[1360] i.e. it would be a question ensuring the correct level of authorisation has been obtained (e.g. in the police

[1361] i.e. the provisions in Chapter II, headed 'Acquisition and disclosure of communications': RIPA, sections 21 to 25

15. A number of leading UK academic lawyers have doubted that Part I, Chapter II of RIPA does apply to SNSs.[1362] However, recently the UK Parliament has amended the definitions in RIPA[1363] to bring internet-based services provided in the UK within the meaning of telecommunications. The terminology used in RIPA – rooted as it is in definitions pertaining to telecommunications – does not immediately seem to lend itself to the basic structure of an SNS service and the communications data between the SNS user and the SNS servers. There have been no reported cases in England and Wales on the application of Part I Chapter II of RIPA to SNSs. Nonetheless, we think that there are various elements which point towards at least reasonable prospects of overseas SNSs being subject to RIPA. The High Court's judgment in the case of *Chambers* [1364] might offer a positive indication of how the courts in the UK would approach this question. Moreover, various committees of the UK Parliament have recorded or expressed views on the applicability of RIPA to SNSs.[1365] Recent legislative amendments of UK data retention law appear to have created a structure whereby overseas-based communications services providers may be required to retain communications data to which designated public authorities in the UK may seek access under RIPA. Although this could clearly potentially include an overseas-based SNS, retention notices are not made public.

16. However, the importance of this is somewhat reduced as far as local authorities are concerned. In practice, in the event of non-compliance by an SNS with a notice to provide communications data, only the Secretary of State may take enforcement action for injunctive or other relief. Moreover, for most law enforcement in the UK, once a suspect's connection to an SNS account is confirmed the focus may well quickly shift to obtaining specific communications data from UK-based communications service providers. The difficulty facing trading standards investigations regarding the latter is lack of power to obtain under RIPA and use traffic data (including IP addresses), which means that TSOs are unable to identify a suspect and or location in the UK from the more basic information that may be provided by an SNS.

Non-compliance

17. RIPA is expressly drafted so as to have extra-territorial effect, which means the UK Parliament intended those designated public authorities to have a legal basis for requesting communications data from overseas-based communications services providers which provide or offer a service in the UK. The problem with this part of RIPA is that whereas some

[1362] We have discussed these at length in the body of our main Opinion
[1363] See Data Retention and Investigatory Powers Act 2014 (as amended) and Counter-Terrorism and Security Act 2015
[1364] *Chambers v DPP* [2012] EWH2 2157 (Admin)
[1365] House of Lords Select Committee on Communications, First Report of Session 2014–15, 'Social media and criminal offences' (London, TSO; 2014) HL/Paper/37
http://www.publications.parliament.uk/pa/ld201415/ldselect/ldcomuni/37/3702.htm
Intelligence and Security Committee, 'Access to communications data by the intelligence and security Agencies' (February 2013) Cm 8514, paras 6-7 and footnote 3:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/225120/isc-access-communications.pdf

communications services providers comply or co-operate with requests for the disclosure of communications data (at least to some extent), others do not and may refuse to respond to RIPA requests at all or deny its applicability to them.

18. The enforcement provisions (i.e. for injunctive and other relief) in Part I Chapter II of RIPA are expressly reserved to the Secretary of State. Unlike some domestic legislation (e.g. Consumer Protection from Unfair Trading Regulations 2008), there are no intra- or extra-territorial offences created by RIPA in respect of refusal or failure to comply with a notice for communications data.

19. In the event of non-compliance, UK law enforcement agencies may still be able to obtain communications data by invoking the arrangements for international mutual legal assistance (MLA) or by way of letters of request from a magistrates' court. Although local authorities are not designated bodies to make direct statutory requests for mutual legal assistance, NAFN may do so on behalf of local authorities through the Home Office. Although it is possible for a local authority to apply for judicial letters of request, we do not envisage the statutory procedure as a practical alternative. We are asked to consider whether local authorities are able to rely on quicker or more direct routes of requesting this information from SNSs.

20. As discussed above, as the law stands, if an SNS provider fails or refuses to comply with a request for "communications data" the harsh reality is that there is very little a TSO is going to be able to do about it.

Judicial approval, criminal threshold & role of NAFN

21. Since November 2012, local authorities have been subject to a requirement to obtain judicial approval for RIPA authorisations. Whilst the continuation of this process is outside of our remit, we note that the Interception of Communications Commissioner has, in his annual reports and other documents including responses to UK Government consultations, consistently doubted the efficacy of the judicial approval process, 'caused confusion, increased their operational costs… and produced no added benefit in seeking to better the scrutiny of applications'.[1366] The Commissioner also expressed concern as to the level of judicial scrutiny. We have been provided with information with our brief which suggests a sharp decrease in the number of RIPA applications progressed by local authorities since judicial approval was implemented in November 2012, which accords with figures obtained by the Interception of Communications Commissioner. In short, budget cuts[1367] combined with the extra administrative burden facing TSOs in complying with judicial approval appear to have contributed to a sharp decline in the number of RIPA authorisations for communications data and accordingly the number of investigations being

[1366] http://www.iocco-uk.info/docs/iocco%20evidence%20for%20the%20investigatory%20powers%20review.pdf
[1367] We are instructed that to national budget cuts of 50% there are further cuts of 25% being forecast by the National Audit Office for the period 2015-16.

carried out. Statistics collated by the Interception of Communications Commissioner suggest many local authorities are now choosing not to use these powers.

22. Having said that, our view is that in the light of relatively recent controversy regarding disproportionate use of RIPA by some local authorities, the criminal threshold, the judicial approval process and the role of NAFN as the SPoC provides effective safeguarding against potentially inappropriate use of RIPA. Going forward, it might be considered that these aspects of recent amendment of RIPA provide the satisfactory safeguards in order to allow local authorities to acquire enhanced powers to investigate criminality in appropriate cases.

Surveillance and covert activity

23. SNS providers such as Facebook allow their users the opportunity to restrict access to their social media content. This can mean that, unlike other online platforms (e.g. advertisements placed on online marketplaces such as eBay), suspected criminality is potentially being conducted otherwise than in a truly open or public setting. Many SNSs provide features which allow users opportunities to limit the audience or categories of persons who have access to content they have added to SNS profiles and group pages. Thus, social media content potentially of evidential value or significant intelligence can effectively be closed off to TSOs and may lead to problems in identifying suspects and gathering evidence of criminality. We have offered within the text of our main Opinion our detailed advice as to when RIPA authorisations are likely to be required in various situations involving both open and public SNS profiles and where more stringent privacy settings have been engaged. We would only reiterate here the comments of the Interception of Communications Commissioner and the risks of failure to obtain RIPA authorisation – particularly where it was due to an 'economy drive' in the light of the financial climate – in the event of an unauthorised, serious breach of an individual's privacy.

Use of powers outside RIPA

24. Guidance issued to local authorities by the Home Office in 2012 makes clear that efforts should not be made to circumvent the constraints of RIPA, including trying to use other statutory powers (e.g. requests for information under the *Data Protection Act 1998*) to obtain communications data unless they expressly provide as such. In our view, local authorities must adhere to this guidance.

25. We have also been asked to consider whether TSOs might use statutory powers to enter premises of an SNS in the UK, seize documents there or request employees or officers to produce documents. In terms of obtaining communications data we do not think this is an option for local authorities in England and Wales given it is known or believed that the electronic data being sought is stored on servers located overseas. Our view is that such efforts would plainly contravene the Home Office guidance and would be outside the ambit

of the powers we have considered. Unlike Part I of RIPA, the statutory powers we have considered are not expressly stated to have extra-territorial application to a legal person such as an SNS provider located outside the UK.

Interception

26. We have been asked to consider whether local authorities can intercept SNS communications. Of course, communications data does not include the actual content of a communication. An investigator may wish to access additional content on an SNS (e.g. for evidence of further offences). The short answer is that RIPA provides that unless authorised by RIPA or any other provision it is unlawful for a person to intentionally intercept communications in the UK in the course of its transmission by postal or telecommunications system otherwise than under warrant issued by the Secretary of State. As the law stands, local authorities cannot obtain an interception warrant under RIPA. Interception is inherently highly intrusive and engages fundamental human rights, including Article 8. The UK Parliament has not deemed it appropriate to designate local authorities to obtain interception warrants and we think it is difficult to objectively balance the necessity and proportionality tests for such activity in the types of trading standards cases we have considered. Quite frankly, unless Parliament makes major changes to RIPA, obtaining an interception warrant is not a viable option in trading standards investigations carried out by a local authority in England and Wales.

Terms of service and onward referral

27. SNSs typically provide terms of service which set out the contractual basis for the relationship between the SNS and the service user. (In the main text of our Opinion we have set out passages from the current Facebook terms of service.) There is clear contractual basis within the terms of service for SNSs to remove or delete criminal or unlawful content, although we are mindful that in practice overseas SNSs may not cooperate or make onerous and burdensome requirements in terms the level of information required. Suspected breaches of copyright and trade marks can also be referred to the individual holders of intellectual property rights. It seems to us that, in cases where communications data cannot be obtained or the administrative burden of obtaining RIPA authorisation for CHIS and / or directed surveillance is deemed prohibitive these steps might be the only effective courses of action that a TSO can take to deal with suspected criminality.

June 2015
Lee J. Reynolds
Justin Amos
Apex Chambers, Cardiff

21 December 2015

UN Special Rapporteurs—written evidence (IPB0102)

1. The UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; UN Special Rapporteur on the rights to freedom of peaceful assembly and of association; and the UN Special Rapporteur on the situation of human rights defenders make the following submission to the Joint Committee of the draft Investigatory Powers Bill, submitted on 21 December 2015. The concerns below have been communicated directly to the Government of the United Kingdom.

2. The Special Rapporteurs welcome efforts of the Parliament of the United Kingdom to initiate a review process aiming towards the adoption of legislation in relation to balancing the collective online rights of the digital community and the need to protect national security and prevent serious and organised crime.

3. We would like to bring to the attention of the Joint Committee on the draft Investigatory Powers Bill a number of specific provisions of the draft Investigatory Powers Bill (from herein the "draft Bill") that are of particular concern, namely in relation to the legitimate enjoyment of the right to freedom of expression and the right to privacy, as enshrined in the International Covenant on Civil and Political Rights.

4. We are especially concerned that, if adopted in its present form, the draft Bill could result in surveillance, including mass surveillance that lacks adequate independent oversight and transparency that will ultimately stifle fundamental freedoms and exert a chilling effect on the rights to freedom of expression and freedom of association.

5. We share the position, outlined in the statement of 4 November 2015, taken by the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, who welcomed the public and legislative scrutiny to which the draft Bill is subject.

<u>Framework for Assessing the Compliance of the Investigatory Powers Bill with International Norms and Standards</u>

6. The Government of the United Kingdom ratified the International Covenant on Civil and Political Rights (ICCPR) on 20 May 1976. Article 19 of the ICCPR protects everyone from interferences with the right to freedom of opinions and protects the right to seek, receive, and impart information and ideas of all kinds, regardless of frontiers and through any media. The right to freedom of opinion is absolute, and no interference, limitation or restriction is allowed.

7. Any restriction on the right to freedom of expression should be narrowly defined and clearly provided by law and be necessary and proportionate to achieve one or more of the legitimate objectives of protecting the rights or reputations of others, national

security, public order, or public health and morals, as provided in Article 19(3) of the Covenant. The UN Human Rights Committee offers an authoritative interpretation of the right to freedom of opinion and expression in its General Comment No. 34 (CCPR/C/GC/34).

8. Analysis relative to the relations between the right to privacy and the right to freedom of expression and opinion under international law is provided by the UN Special Rapporteur on freedom of expression in his report on the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression (A/HRC/23/40); his report on the use of encryption and anonymity to exercise the rights to freedom of opinion and expression in the digital age (A/HRC/29/32); his report on the protection of sources of information and whistle-blowers (A/70/361); as well as by the UN High Commissioner for Human Rights in his report on the right to privacy in the digital age (A/HRC/27/37).

Clauses of Concern in the draft Investigatory Powers Bill

9. The clauses of the draft Bill that cause concern from the perspective of the rights to freedom of opinion and expression and freedom of association include at least the following:

Clause 61 on the authorisation of warrants for journalists' communications data

10. *Clause 61* of the draft Bill establishes the authorisation procedure for officials to execute a warrant for collecting communications data for "identifying or confirming a source of journalistic information". Under *Clause 61(7)*, a "source of journalistic information" refers to "an individual who provides material intending the recipient to use it for the purposes of journalism or knowing that it is likely to be so used." After the warrant has been approved by a designated senior official of a relevant public authority, such authorisation must be obtained from a Judicial Commissioner. *Clause 46(7)* provides the reasons for which a Judicial Commissioner may authorise a warrant where it is necessary and proportionate, including "national security," "public safety," "preventing disorder," assessing and collecting taxes, and "for the purposes of exercising functions relating to … financial stability." Additionally, the authorities are not required to give notice of such request or authorisation to the subjects of a warrant for communications data or their legal representatives. Further, the draft Bill exempts the intelligence services from seeking approval for obtaining journalistic information.

11. The purposes for which a warrant for communications data may be executed are vague and not tethered to specific offences. Consequently, the Judicial Commissioner may enjoy authority to approve surveillance beyond the narrow range of circumstances where it would be necessary and proportionate to achieve one or more of the legitimate objectives of protecting the rights or reputations of others, national security, public order, or public health and morals, as provided under article 19(3) of the ICCPR. Also, the authorities' discretion to withhold notice of such

surveillance would deprive individuals and associations of their ability to challenge suspect or illegal surveillance, even after the warrant for such surveillance has been executed and the investigation closed. The exemption of the intelligence services from seeking approval for communications data warrants, would effectively allow the Government to obtain communications data for intelligence purposes without any external or independent oversight. Further, it is unclear who may be deemed "a source of journalistic information". Such definition does not clarify whether these warrants could encompass information provided by non-traditional news sources, such as civil society organisations, academic researchers, human rights defenders, citizen journalists and bloggers. Such provision may stifle the right to freedom of expression, while also resulting in a chilling effect on its legitimate exercise.

Clauses 71 to 73 on notices for the retention of communications data

12. *Clause 71* permits the Secretary of State to issue a notice requiring telecommunications operators to retain "relevant communications data" for a maximum of 12 months. Under *Clause 71(9)*, such communications data include information identifying the sender, recipient, time and duration of the communication and internet protocol addresses. The Secretary of State may issue such notices as long as they deem retention "necessary and proportionate" for a range of purposes, including "national security", "public safety", "preventing disorder", "assessing and collecting taxes" and for "exercising functions relating to… financial stability". Under *Clause 73(10)*, the Secretary of State may decide the review after considering the conclusions of the Technical Advisory Board and the Commissioner. *Clause 77(2)* states that a "telecommunications operator, or any person employed for the purposes of the business of a telecommunications operator, must not disclose the existence and contents of a retention notice to any other person."

13. The procedure and reasons for the retention of communications data in the draft Bill are vague and could permit the Secretary of State to require third party data retention that is excessive and disproportionate. The process lacks any meaningful independent oversight, and while the Secretary of State has a duty to consult the Board and the Commissioner, their conclusions are not binding and the Secretary of State retains unilateral authority to vary, revoke or confirm the terms and conditions of the notice. The prohibition on telecommunications operators to disclose data retention notices may deprive affected customers of their right to challenge the retention of their data, even after such notice has expired and the investigation concerning such data has been closed.

Clauses 106, 107,109 and 112 on bulk interception warrants

14. *Clause 106* provides that intelligence services may apply for a warrant to intercept communications and related communications data in bulk "in the course of their transmission by means of a telecommunication system." Such action may be authorised where the "main purpose" of the warrant must be to intercept communications and related or communications data that are sent to or received by

individuals "outside the British Islands." Additionally, under *Clause 107*, the warrant must be "necessary" to serve at least one of three purposes: the "interests of national security"; the interests of national security and "for the purposes of preventing or detecting serious crime"; or the "interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security" and provided that the information sought to be obtained relates to "the acts or intentions of persons outside the British Islands". Under *Clauses 107 and 109*, such warrants must be issued by the Secretary of State and approved by a Judicial Commissioner respectively. Under *Clause 112(1)*, a bulk interception warrant is valid for a maximum of six months. However, at any time before or once the warrant expires, the Secretary may renew it subject to the procedures described above.

15. Similar to the criteria for authorising warrants for journalists' communications data, the provisions on bulk interception warrants are vague and not tied to specified offences, and include ambiguous terms such as "economic well-being", heightening the risk of excessive and disproportionate interception. Further, the power to renew bulk interception warrants indefinitely is not a meaningful limit on the duration of these activities, which is a critical safeguard against undue interferences with the rights to freedom of expression and privacy.

Clauses 189 to 191 on powers to require the removal of electronic protection

16. Under Clause *189(4)(c)*, the Secretary of State may make regulations imposing obligations on telecommunications operators "relating to the removal of electronic protection applied by a relevant operator to any communications or data." *Clause 189(6)* authorises the Secretary to issue a technical capability notice requiring an operator to "take all the steps specified in the notice for the purpose of complying with those obligations." For operators outside the United Kingdom, such notice may require "things to be done, or not to be done, outside the United Kingdom." *Clauses 190(3) and 191* establish criteria for issuing and challenging technical capability notices that are materially similar to those for data retention notices described above and *Clause 190(8)* prohibits the subject of technical capability notices from disclosing the "existence and contents of the notice to any other person".

17. The lack of substantive limits on the Secretary of State's power to establish regulations may interfere with the ability of telecommunications operators to protect their users' communications through end-to-end encryption. In particular, the broad discretion to regulate might lead to blanket restrictions on encryption that affect massive numbers of persons, which would most likely result in a breach of the requirements of necessity and proportionality. The ambiguous purposes permitted to authorise the removal of electronic protections and the non-disclosure of such measures also raise the concerns listed above with regard to *Clauses 71 to 73*.

Clauses 167 to 168 on the appointment of Judicial Commissioners

18. Under *Clause 167*, the Prime Minister appoints Judicial Commissioners, in consultation with various ministers specified and the Investigatory Powers Commissioner (the head of the Judicial Commissioners). Judicial Commissioners are also required to hold or have held a high judicial office. Each Judicial Commissioner is appointed for a term of three years under *Clause 168*, after which the Prime Minister may reappoint a Judicial Commissioner for another term. This power is vested exclusively in the Prime Minister, without input (consultative or otherwise) from the Parliament, judiciary, or any other independent body in the vetting or approving candidates.

19. The power to appoint the Judicial Commissioners compromises the independence and impartiality of the Judicial Commissioners, who oversee the surveillance procedures outlined in the draft Bill.

Concerns with the process of pre-legislative scrutiny

20. The Special Rapporteurs would also like to raise concerns about the review process of the draft Bill, which reportedly fails to provide civil society, the private sector, the technical community and all interested stakeholders with sufficient time to provide meaningful input on such a comprehensive draft Bill.

Concluding Observations

21. We appreciate the importance of this effort to place certain investigatory powers under the sanction of a clear and consistent legal regime governed by the rule of law. Nonetheless, we wish to express serious concern that the above-mentioned provisions of the draft Investigatory Powers Bill, in its current form, contain insufficient procedures without adequate oversight and overly broad definitions that may unduly interfere with the rights to privacy, freedom of opinion and expression and freedom of association, both inside and outside of the United Kingdom, as provided under articles 17, 19 and 22 of the ICCPR.

22. We urge the Joint Committee on the draft Investigatory Powers Bill to take all steps necessary to conduct a comprehensive review of the draft Investigatory Powers Bill to ensure its compliance with applicable international standards as outlined in this submission.

21 December 2015

Virgin Media—written evidence (IPB0160)

Introduction

Virgin Media Limited ('**Virgin Media**') welcomes the opportunity to respond to the Joint Committee's call for written evidence in its scrutiny of the draft Investigatory Powers Bill (the '**IPB'**). We agree that this is an extremely important draft Bill that will govern the use and oversight of investigatory powers by law enforcement and the security services for many years to come.

Virgin Media is an entertainment and communications business which offers a range of services to consumers, and to business customers through its group companies such as Virgin Media Business. In particular, Virgin Media provides high speed broadband, fixed line telephony, mobile telephony and programming services to consumers in the UK, as well as public Wi-Fi services, for example on the London Underground. Virgin Media is a wholly owned subsidiary of Liberty Global, an international cable operator with operations in 14 countries including 12 in Europe.

Virgin Media believes that law enforcement authorities should have the benefit of reasonable and appropriate investigatory powers in order to help with the detection and investigation of crime and to safeguard national security. However, this has to be balanced against the need to protect customers' privacy. The potential for intrusion into privacy under this draft Bill is significantly greater than under the legislation it is intended to replace. We believe it is for Parliament to decide where the balance should lie between privacy and intrusion, and that any legislation governing investigatory powers should ensure that:

(a) the balance struck between privacy and intrusion is lawful (notably under the Human Rights Act and the European Union's Charter of Fundamental Rights), appropriate and justified;
(b) the legal obligations placed on communications service providers ('**CSP**s') are clear;
(c) the legal obligations are technically feasible and do not place the network or customers of a CSP at risk;
(d) the appeals and oversight mechanisms are sufficiently robust to ensure the lawful and proportionate use of investigatory powers; and
(e) measures imposed do not damage the competitiveness of UK organisations subject to the obligations in what is an increasingly global marketplace.

Virgin Media's response will focus on the potential practical implications for a CSP, should it become subject to any of the obligations set out in this draft Bill.

Summary of Written Response from Virgin Media

1. The scope of the investigatory powers permitted under the new Bill is not clear. In particular as currently drafted CSPs may be required to retain third party data. We believe that any requirement to retain third party data should be excluded from the

draft Bill and made subject to further consultation and Parliamentary approval if required at a later date.

2. The Bill should make clear what is meant by an ICR and whether this includes any third party data. We believe retention of Internet Connection Records ('**ICRs')** may be technically feasible but is likely to be complex and costly. The exact detail of what CSPs should retain and how needs clarification as soon as possible.

3. The principle of full cost recovery should be written into the Bill. This will act as an incentive to government and law enforcement authorities to limit requests to what is necessary, reasonable, proportionate and cost effective.

4. We welcome the creation of the new Investigatory Powers Commissioner ('**IPC'**) and believe there should be a single regulator for investigatory powers. Where the ICO retains some responsibility in respect of investigatory powers, the boundaries need to be clarified and we recommend its powers are delegated to the IPC to avoid overlap and conflict and realise efficiencies inherent in having a single regulator.

5. Oversight: we believe a 'double-lock' authorisation and approval process should apply to any retention notice, national security or technical capability notice imposed on a CSP following the consultation and review processes. Clarification is also needed to ensure Judicial Commissioners can review the necessity, proportionality and reasonableness of a particular measure, with full access to the evidence.

6. Clarification is needed as to the scope of the technical capability notice and its possible impact on CSPs ability to provide encrypted services and whether CSPs could be required under such a notice to provide encrypted third party data 'in the clear'.

7. Authorisation of any Equipment Interference ('**EI'**) warrant or technical capability notice needs to take into account the potential impact on customer privacy and security and the security, resiliency and availability of a CSP's network. CSPs should not be held responsible for breach of a legal obligation where that breach was caused by compliance with an EI warrant or technical capability notice. CSPs should also be permitted to disclose the impact of the EI warrant or capability to Ofcom and/or in defence of any legal proceedings brought against it as a result of an alleged breach of its other legal obligations. The oversight mechanism needs to take into account any concerns a CSP may have, particularly in relation to the privacy and security of its customers and the security, resiliency and availability of its network and include an appeals mechanism for CSPs.

8. We welcome the proposal to place bulk powers on a clear statutory footing and therefore open to debate and consideration by Parliament. If such powers are required, we believe they should be used only where necessary and proportionate. We welcome the double lock oversight applied to such powers, although we believe the scope of this oversight mechanism needs to be clarified as described above.

9. This draft Bill includes sweeping extraterritorial powers which in many cases will not be enforceable. We believe the government should prioritise mutual legal assistance treaties to ensure co-operation.

10. Request filter: it is difficult to comment in any detail on the implications as the Bill only includes enabling provisions. Use of a request filter may help to protect privacy by limiting the results presented to law enforcement but the power and intrusiveness of such a tool is likely to be considerable, enabling complex queries of multiple data stores. It is not clear exactly how concerns expressed by the Joint Committee on the Communications Data Bill 2012 in relation to the request filter will be addressed.

11. The draft Bill should not introduce the ability for police to bypass SPOC consultation in the event of an emergency. This jeopardises security, introduces inefficiencies and is not necessary. Emergencies can and should be dealt with by LEAs sharing the use of SPOCs to ensure 24x7 cover.

Section 1: Scope and Third Party Data

Virgin Media supports the conclusions of David Anderson QC's recent review of investigatory powers where he recommended:

"*A comprehensive and comprehensible new law should be drafted from scratch, replacing the multitude of current powers and providing for clear limits and safeguards on any intrusive power that it may be necessary for public authorities to use.*"

We welcome reform of the current, outdated statutory regime and the attempt to bring the majority of investigatory powers into one single Bill. In our view the new Bill is comprehensive, but as a consequence of the intention to ensure the Bill is technology neutral and future-proof, the extent of the investigatory powers permitted under the new Bill is not clear. We believe Codes of Practice will assist in determining what is content and what is 'retainable' communications data, but details of what measures may be demanded of CSPs will not become clear to CSPs until after appropriate notices (if any) are issued under s71, s188 and 189 of the Bill. The draft Bill has the capability to be wider in scope than continuation of existing powers, such as the existing data retention regime, with the addition of Internet Connection Records and it is possible that the scope of these powers and how they may change over time will not be known to Parliament or the public.

By way of example, the Home Secretary in introducing this draft Bill made clear that this is "*not a return to the Draft Communications Data Bill of 2012. It will not include powers to force UK companies to capture and retain third party internet traffic from companies based overseas….*"

However, changes to the definition of "communications data", coupled with the power to require a provider to "generate" data for the purposes of retention, mean that a future Home Secretary could in theory do exactly that, without a return to Parliament. In our view

s71(9) of the Bill should be modified so that 'relevant communications data' should relate only to data processed by a CSP in order to provide a service to customers in the UK and not to data simply transiting the network with no activity undertaken upon it, for reasons highlighted below and in Section 2 and Section 6.

Graham Smith in his written evidence to the Science and Technology Committee (IPB0025) set out with clarity how the definition of "communications data" in the draft Bill differs from the definition in the Data Retention and Investigatory Powers Act 2014. In particular, as he pointed out at paragraph 27:

"Previous UK data retention obligations under DRIPA and its predecessor have required only the retention of data generated or processed in the UK in the course of providing the service. They have articulated no power to require data to be created for the purpose of retention."

We also refer you to paragraph 13c of Anderson QC's report:

"There should be no question of progressing proposals for the compulsory ***retention of third party data*** *before a compelling operational case for it has been made out (as it has not been to date) and the legal and technical issues have been fully bottomed out."*

We agree with Anderson QC's conclusions and note that none of these concerns have yet been addressed.

Section 2: Internet Connection Records

The proposed requirement to retain ICRs was discussed in some detail at the session on 9th December and the session on 14th December. As discussed in those sessions, we believe the retention of some form of ICR is technically feasible, but a number of questions remain to be answered. In particular:

(a) ICRs are not clearly defined in the draft Bill (there appear to be two different definitions, neither of which make clear exactly what data needs to be captured and stored to create the ICR);

(b) ICRs are not a recognised data set and not something created or retained by CSPs for their own business use. They would have to be created from a variety of data sources which are still to be determined; and

(c) Until we determine what is an ICR, how the ICR is to be captured and stored and then made available for disclosure, it is not possible to give a reliable estimate of the likely costs, but we believe they are likely to be significant.

The key elements to consider in determining the likely complexity and costs will be:

(a) The data sources, how the data will be captured, whether capture of content to strip out relevant communications data is required or can be avoided and whether any data is encrypted;

(b) What exactly is being stored and the volumes of data to be stored – and for how long;

(c) Space and power for hardware necessary for capture and storage;

(d) Whether the capture method has any impact on performance of the network and how this can be mitigated;

(e) Ongoing operational and maintenance costs for new systems; and

(f) How the data will be made available for disclosure.

These same technical challenges and more will apply to any requirement to retain third party data. In particular a CSP may have to capture communications data from content, which may or may not be encrypted. We question whether it would be technically feasible to capture the data, but even if it is, the CSP would not be able to verify the accuracy of that data, so it may have limited evidential value. As such we believe retention and disclosure of third party data has more in common with interception of content. If the conclusion is that the Bill must include a power to require the retention of third party data, we believe it would be more appropriate to treat it as an interception capability and the approvals mechanisms for disclosure should be the same as for interception of content.

Section 3: Oversight

We welcome the creation of the Investigatory Powers Commissioner, replacing the three existing bodies. Having one single regulator responsible for authorisations, inspections and audit is likely to increase efficiency and build up significant expertise. However, in that context we note that under the draft Bill the Information Commissioner's Office (the '**ICO'**) retains responsibility for auditing the security of CSP retention infrastructure. In our view this audit responsibility should be formally delegated to the IPC who will have extensive audit rights and considerable knowledge of any infrastructure. We believe this is the best approach to ensure security of the retained data.

The potential conflict between the powers of the ICO and the powers of the new IPC arise again in relation to error reporting. CSPs are required to report errors under the new Bill to the IPC and the same errors to the ICO as personal data breaches under the Privacy and Electronic Communications (EC Directive) Regulations 2003 ('**PECR'**). We believe this conflict needs to be considered and addressed in the legislation so that errors properly reported to the IPC, a regulator with all necessary oversight powers, will be sufficient. Reporting also needs to be anonymised in the manner adopted by the Interception of Communications Commissioners Office ('**IOCCO'**), otherwise it creates a real operational risk that: (a) CSPs subject to notices; and (b) details of operational activities, may become known to targets and thus jeopardise law enforcement investigations.

We welcome the "double-lock" approvals process in respect of warrants and the assurances received from the Home Office and during oral evidence sessions that this process would

allow for the IPC to consider necessity and proportionality with all of the evidence before them – not merely to determine whether the Secretary of State had followed the correct procedure. We believe this is an extremely important safeguard and this intention should be made clear on the face of the Bill. It is not clear on current drafting.

The draft Bill retains an internal authorisations process for the acquisition of targeted communications data as set out in current legislation. We are unclear why the 'double-lock' pre-approvals process does not also apply to the acquisition of targeted communications data and the imposition of a retention notice, technical capability notice or national security notice, including any amendments of requirements as a result of new services being offered or changes to existing services by a CSP. We believe that it should.

The CJEU is currently considering the question of whether judicial/independent approval is required in relation to disclosure of communications data (following a referral from the Court of Appeal in the Digital Rights Ireland case). If the CJEU finds that judicial approval is not required, and the volume of requests makes it impractical for the IPC to pre-approve all requests for targeted communications data, then we believe the IPC should as a minimum pre-approve all retention notices under s71, any national security notices under s188 and technical capability notices under s189, including any amendment to such requirements. Although we welcome the process for review by the Secretary of State set out in s73 and s191 of the draft Bill, with obligations to consult the Technical Advisory Board and the IPC, the final decision rests with the Secretary of State. We believe a double-lock process could be applied to the Secretary of State's decisions in these cases, with a right of appeal for the CSP where a notice is to be imposed despite a CSP's objections and after the review process has been exhausted. A robust review and appeals process is of particular importance given the extensive nature of the potential obligations that could fall within the scope of s188 and 189 of the draft Bill, the amended scope of communications data retention and the extensive extraterritorial reach of these obligations.

The draft Bill includes some other inconsistencies. As drafted, the IPC is responsible for keeping under review national security notices but not technical capability notices. We believe the IPC should be responsible for keeping both under review and also any applicable retention notices under s71.

In addition we recommend that the role of TAB is extended to include analysis not only of technical feasibility and costs of any measures, but also give views on the proportionality of such measures in that context.

Section 4: Equipment Interference

We welcome the proposal in the draft Bill that equipment interference warrants be subject to increased safeguards in the form of the double-lock authorisation and approval process. However, we have a number of key areas of concern in relation to equipment interference:

(a) The potential impact on the privacy and security of our customers, the integrity and security of our network and the availability of services to customers;

(b) The extent to which the draft Bill may require a CSP, and therefore its employees, to assist with EI; and
(c) The potential costs of implementing EI.

The measures CSPs take to protect the personal data and security of their customers have come under significant scrutiny. CSPs have a commercial and reputational imperative to protect the personal data and security of its customers, which is backed up by legal obligations such as those under the Data Protection Act 1998 (soon to be replaced by the EU General Data Protection Regulations) and PECR. CSPs in the UK and Europe also have obligations to ensure the security and resilience of their networks and maintain availability to end users under Articles 13a and b of the Framework Directive (implemented in the UK as s105A-D of the Communications Act 2003).

Implementing an EI warrant (or maintaining a technical capability to do so) will conflict with these imperatives and the CSPs legal obligations if for example it undermines customer or network security or brings down part of the CSPs network. We believe that CSPs would also be prevented from explaining that the EI warrant or capability was the reason for the breach, due to the operation of s102 of the draft Bill.

The role of CSPs in EI is not made clear in the draft Bill. We believe there needs to be full consultation with CSPs in advance of any EI warrant or technical capability notice being imposed, for example to guard against EI having a negative impact on networks or customers. As drafted, no consultation appears to be required before the imposition of EI warrants. The draft Bill also creates the possibility CSP's employees may be required to actively assist in EI operations, perhaps to seek out vulnerabilities for exploitation or develop vulnerabilities, which we do not believe is appropriate.

We are also concerned about the potential costs of implementing EI, both in terms of implementation of capability – which we are unable to estimate on current information – and in terms of potential legal exposure to fines and damages.

Recommendations:

(a) Authorisation of any EI warrant or technical capability notice needs to take into account the impact on security, resiliency and availability and CSPs should be able to contribute to this process;
(b) CSPs should not be held responsible for breach of a legal obligation where that breach was caused by compliance with an EI warrant or technical capability notice. CSPs should also be permitted to disclose the impact of the EI warrant or capability to Ofcom and/or in defence of any legal proceedings brought against it as a result of an alleged breach of its other legal obligations;
(c) We believe that a strengthened authorisation and appeals process as described in Section 3 is important in relation to EI warrants and technical capability notices relating to EI measures;
(d) There should be consultation with CSPs in advance of any measures being implemented but CSPs should not be required to take a direct role in EI operations,

for example to seek out or develop vulnerabilities as part of any technical capability notice.

Section 5: Maintenance of technical capability

This power is more broadly drafted than the provision it replaces, s12 of RIPA, which requires those CSPs issued with a notice to maintain interception capability. At this point in time we are unable to offer much meaningful comment since the power is open-ended and therefore we are not clear what capability CSPs may be required to maintain under s189. We would like to see more clarity in the Bill specifying what CSPs may be required to do. For example, could CSPs be prevented from offering customers services which benefit from end to end encryption? Could CSPs be prevented from offering customers VPN services? Such prohibitions may help to secure the retention and disclosure of communications data but we question whether these measures are necessary, proportionate and reasonable. If s189 remains broadly drafted, then we recommend introducing a strengthened authorisation or appeals process in addition to the consultation and review process set out in s189-191 of the draft Bill, for instance as described in Section 3 above.

Unlike the provision it replaces, a technical capability notice may apply to private as well as public networks and services. We agree that investigatory powers should apply to over the top (OTT) services, as we believe the data should be obtained from the provider who is providing the services (and who is therefore closest to the data in question). However, we are concerned that the powers may be used instead to require a CSP who provides private networks to businesses and wholesale services to become a 'one stop shop' for this data. This is problematic for the reasons set out in Section 1, Section 2 and Section 6.

Section 6: Cost Recovery

The Bill states that there will be appropriate contribution to costs as determined by the Secretary of State, which shall not be nil. We believe the draft Bill should include a clear commitment to ensure full cost recovery. Cost recovery acts as an incentive to government and law enforcement authorities to limit requests to what is reasonable, proportionate and cost effective. This is particularly important here since the requirements that may be imposed are not made clear on the face of the Bill. In addition, the new Bill changes the landscape by including the power to require CSPs to generate and retain to high security standards data which the CSP would not have created or retained for its own business purposes.

If the Bill does not provide protection for full cost recovery, those CSPs who are subject to such obligations (and who therefore may at some point be required to pay to implement these measures even though they are not requested by customers or needed to provide the service) are placed at a significant competitive disadvantage in comparison with entities who are not subject to similar obligations or who can incorporate overseas to avoid enforcement of such obligations. We believe that a system of full cost recovery, both in terms of capital expenditure and operational expenditure, is important to avoid distortion in the marketplace and provide a commercial incentive for government and law enforcement

authorities to limit both the requirements for system builds and disclosure requests to what is necessary.

Section 7: Bulk capabilities

We welcome the proposal to place bulk powers on a clear statutory footing and therefore open to debate and consideration by Parliament. If such powers are required, we believe they should be used only where necessary and proportionate. We welcome the double lock oversight applied to such powers, although we believe the scope of this oversight mechanism needs to be clarified as set out in Section 3.

Section 8: Extraterritorial application

We are concerned by the inclusion of sweeping extraterritorial powers which in most cases will not be enforceable, giving a misleading impression that overseas companies will be subject to the same obligations as UK companies. We believe the government should prioritise the implementation and use of mutual legal assistance treaties (MLAT) and the investigatory powers set out in this draft Bill should only be used (if at all) in respect of services provided by overseas providers to the extent they are provided to UK customers.

Section 9: Request Filter

The provisions in the draft Bill appear to be little more than enabling provisions, so it is difficult to comment in any detail on the implications. However, we have had some engagement with the Home Office and we understand that the intention is for a request for data to be passed through the filter to ensure that only the relevant data is passed on to law enforcement. If operated in this way it should help to protect privacy. However, the power and intrusiveness of such as tool is likely to be considerable, enabling complex queries of multiple data stores. Clarification around scope, controls, security, oversight and implementation is required either on the face of the Bill or in secondary legislation. It is not clear how exactly concerns expressed by the Joint Committee (Communications Data Bill 2012) will be addressed. Nor is it clear to what extent the filter and any results will be audited and how errors will be reported.

We welcome the obligation on the Secretary of State to consult the IPC as set out in s51(5) but suggest that as well as an obligation to consult, there should be a double-lock approvals process in respect of implementation and use of the request filter.

Section 10: Use of SPOC in an emergency

The SPOC (single point of contact) process was much praised by CSPs in their response to the Anderson review. SPOCs are knowledgeable about the data available to law enforcement and how that data can be used. They have been fully trained and accredited and they operate as a quality and process filter. However, the Bill introduces an exception to be used in an emergency which allows the police to bypass SPOC consultation. This is not necessary or good practice. We believe that emergencies can be dealt with through LEA co-operation agreements to share the use of SPOCs to ensure 24x7 cover. If a police officer is

able to bypass a SPOC, then all the controls set up to: (a) ensure an appropriate request is made in the manner most likely to result in disclosure of relevant data; and (b) ensure data is only disclosed to authorised individuals; will also be bypassed. We believe this is a very important safeguard, and its removal creates an unnecessary security risk.

14 January 2016

Philip Virgo—written evidence (IPB0061)

Personal Background

1) I organised the EURIM (Digital Policy Alliance), scrutiny of RIPA, the EURIM-IPPR Partnership Policing study and a number of more recent exercises looking at practical co-operation, for example in the aftermath of the 2011 London Riots. I also have various current relevant professional, political and voluntary roles.

2) I have also submitted evidence to the Science and Technology Select Committee inquiry into the technology aspects of the Bill . That evidence is very relevant to the points I make below and I hope that the Scrutiny Committee will cross refer to it as necessary - particularly to the appendix, "Observations on the Draft Investigatory Powers Bill", contributed by Chris Sundt, sometime chief security architect for ICL, a consultant to GCHQ for many years and industry representative on the Strategy Board for the National High Tech Crime Unit.

Summary

3) The deficiencies of current legislation were well demonstrated during the London Riots of 2011 when events moved faster than authorisation processes and law enforcement was unable to make effective use of more than a fraction of the information that communications service providers were making available on a voluntary basis, paperwork to follow.

4) It is more important to provide democratically accountable governance for voluntary co-operation between industry and law enforcement, using the ability of the former to rapidly filter information in time for instant decision-taking (as when checking the location and pattern of use of a smartphone before authorising a financial transaction), than to make arrangements for the compulsory storage of yet more information, in case it might be of intelligence value.

5) The accelerating rate of change of communications architectures, let alone technologies, makes it essential for legislation covering investigatory powers to be based on objectives and principles rather than the structure of BT's current communications network. Any attempt to "define" the services covered, data to be collected and technologies envisaged is likely to be out-of-date before the legislation is implemented, unless the legislation is used to help prevent change, thus putting the UK at serious competitive and economic disadvantage.

6) The volume of communications and related data is expanding rapidly with ubiquitous smart devices communicating over a growing range of channels, almost all capable of being used for criminal purposes. Most will never be worth covering, but it is essential to avoid "tipping off" criminals on how to evade surveillance. ***The regime should therefore apply to ALL types of communications service provider, with reimbursement processes which cover the full cost, including to small community broadband operators or wifi providers whose users might include those whose activities merit active and ongoing surveillance.***

7) The biggest cost is not recording or retaining data, but keeping it secure in the world's biggest set of "honeypots for hackers". Many of those with current investigatory powers delegate these to junior staff and/or have already been warned or fined by the Information Commissioner's Office. Those given Investigatory Powers should be required to maintain single points of contact, with security processes that are fit for purpose.

8) ***The penalties should be substantial for organisations exercising powers under the legislation which fail to keep data secure, not just for staff who actively abuse their powers.***

9) My responses to the questions on which the Committee is inviting evidence are:

A. To what extent is it necessary for the security and intelligence services and law enforcement to have access to investigatory powers such as those contained in the draft bill?

10) Legislation regarding information technology and electronic communications needs to be technology neutral lest it become outdated before it is implemented. The problems of identifying which services might carry information of value to law enforcement or the security services, let alone of securely storing unfiltered data in case it is needed (honeypots for hackers) are becoming harder every year.

11) The growth of device and transaction tracking services in support of adware and other forms of spyware has resulted in an explosion of short messages, whether or not devices are in active use by a human, with each “user controlled” transaction, message or site visit potentially triggering dozens of monitoring and tracking messages, plus further streams of messages even when the user is not consciously using the device . This will become worse with the “Internet of Things” with large numbers of other machine generated communications.

12) Most “utility” service providers have no interest in, or means of identifying, which is which. If requested they would therefore need to retain all or install filtering equipment. The cost of doing so could dwarf currently estimates, except on the part of those communications services which filter out adware and tracking software in accordance with customer wishes, thus incurring the wrath of those whose business models are now underpinned by adware/spyware revenues .

13) Meanwhile the range and variety of channels over which Internet message and transactions may travel are proliferating. Fixed, mobile and wifi communications services are converging. The BT local loop and backhaul monopolies are breaking down. There is a strong growth of traffic which bypasses IPV4 addressing bottlenecks (let alone “traditional” Tier One surveillance points), albeit mainly for local machine to machine communications (e.g. for smart building, transport, telecare etc. devices).

14) It is clear that intention is for this legislation to cope, at least in part, with such change, The 'FactSheet' on Internet Connection Records (ICRs) states that "...without the

retention of ICRs, resolving an IP address back to a single user will often not be possible as multiple users may be associated with that IP address." The implication here is that ICRs hold not just IP addresses but other information that can be used (with varying degrees of reliability) to identify specific devices, their location and, by extension, their users. ICRs are to be captured by the network access provider "...e.g. the Internet Service Provider or Wi-Fi operator...".

15) This suggests that ICRs might be demanded from, not just large or small ISPs, but also from schools, universities, libraries, banks, coffee shops, community centres and anyone else providing (semi-) public internet access. If this is the intention then the cost and security implications are massive. If it is not the intention, then such public access points provide a simple way for those of nefarious intent to by-pass the system.

16) Either way, ***assuring users that their communications are not liable to surveillance is surely "tipping off" and should thus be as much an offence as telling them that they have been targetted.*** The idea that small ISPs do not need to worry because they are most unlikely to be of "interest" undermines the basis of the legislation because it is easy to envisage circumstances in which community ISPs serving inner city estates or leafy suburbs ***should*** be of interest, whether as centres of organised crime or terrorism or both.

17) Meanwhile technologies such as Tor and Freenet and the adoption of VPNs to proxies in other jurisdictions provide increasingly accessible ways for the hardest and most dangerous targets to bypass "traditional" systems monitoring Tier One (also a fluid definition) communications providers. The necessity and proportionality of inevitably ineffective population-scale surveillance is not credible.

18) ***We can therefore expect a trend towards granular (location and/or service) access, with most communications service providers not required to retain data at any time but even modest operators required to do so when they are identified as serving targets or communities of interest.***

19) If so, the legislation should be generic with a "guarantee" to cover the full costs, including of keeping data secure, incurred by any service provider (large or small) required to retain data. Such an approach will present obvious problems to those wishing to exercise powers under the bill but that would give them an incentive to ration their use of those powers***.***

B. Are there sufficient operational justifications for undertaking targeted and bulk interception, and are the proposed authorisation processes for such interception activities appropriate and workable?

20) There is a need to distinguish between the value of providing more efficient and accountable authorisation processes for undertaking targeted and/or bulk interception and the value of storing large volumes of data in case in might be needed.

21) There are growing concerns that government and law enforcement agencies (especially those outside the core intelligence services) do not secure data adequately. The number of local authorities suffering data breaches (according to the Information Commissioners' Office) illustrates that is a serious problem among many of those with investigatory powers.

22) ***The clauses concerned with unlawful access to data in Part 1 need to be extended to cover the failure to adequately secure retained data, particularly claimed under warrant, notice or authorisation. Penalties should be linked to, but significantly more severe, than those under Data Protection legislation and cover anyone in industry or government holding such data.***

23) A more serious flaw is that the Bill still does not address the organisation of practical co-operation in time to meet operational needs, as occurred during the London riots, when law enforcement was unable to make effective use of the information streams on offer from mobile operators and ISPs. Here ***the need is for access to the real-time computing power of industry in time to make a difference and save lives***. This raises problems of governance more profound and difficult than those covered in the bill.

24) The arguments around the current Microsoft/Department of Justice case concerning access to Hotmail boxes in Ireland are relevant because the original request to Microsoft was allegedly because the mutual assistance process is too slow and cumbersome. There are serious cross-border problems, including between police forces in the UK let alone across the EU or globally, in an age where communications recognises no jurisdictional boundaries international law just has not caught up.

25) The extra-territoriality clauses in the draft Bill are unlikely to help sufficiently to make a material difference. ***The need is to make voluntary co-operation, including across borders, very much easier***. Thus during the London Riots a communications service provider in North America obtained a local warrant which enabled it to legitimately decrypt communications between gang leaders before UK law enforcement was able to work out how to organise a request.

26) ***The current pressures on police budgets mean that their ability to act as the first line of defence in addressing cyber-crime or terrorism depends on making practical progress with implementing the recommendations for Partnership Policing made by EURIM and IPPR a decade ago*** This is particularly so with regard to the governance of co-operation between industry and law enforcement to provide, for example, ***voluntary*** filtered real-time access to communications and transactions in time to help prevent, not just investigate, criminal activity.

C. Should the security and intelligence services have access to powers to undertake targeted and bulk equipment interference? Should law enforcement also have access to such powers?

27) The security and intelligence services should not be given the power to distort the growth and competitiveness of the UK communication market by routing traffic through BT (or other) bottlenecks which they can monitor. They should, however, have access to the power to use the monitoring facilities inherent in most communications equipment, without the need to specifically inform the relevant service provider, who might be quite small (see paras 15 and 16 above).

28) There is a need to ***remove concerns over the potential cost (including monitoring and storage equipment and security costs that would not otherwise be needed) and also over the effect on network performance, as well as costs, (if traffic has to be routed through monopoly bottlenecks where it can be monitored and stored at HMG expense).***

29) If this is not addressed, the cost to the economy caused by such concerns (e.g. delayed and distorted investment in communication infrastructure and services) is likely to be far greater than any estimates currently envisaged.

D. The need to use investigatory powers to help rebuild public confidence in the on-line world

30) There is a need to look at the potential for the legislation to lead to more effective co-operation between the security services, law enforcement agencies and communications and Internet service providers in identifying and removing on-line predators (from pederasts to fraudsters). Far from encouraging improvements in co-operation or reducing the number of organisations with "snooping powers", the Bill appears to increase them. That may, however, be because RIPA did not supersede the existing powers of organisations not included in its schedules and the new Bill is more comprehensive.

31) If Bill does indeed cover ALL existing investigatory powers, then the time has come to also implement one of the ideas discussed in the margins of RIPA. This was that ***ALL those with investigatory powers should route their requests through a "Single Point of Contact" (SPOC) whose staff have been trained in their duties, including to keep the results secure. The security requirement should include physical inspection (not just a paper validation of theoretical processes). Those without a SPOC, trained staff and adequate security should lose their powers and be required to route requests through an organisation which can meet the requirements.***

32) The welcome inclusion of penalties for the abuse of the powers does not address the problem of Councils giving powers to dozens of staff, from senior to junior or lacking the procedures to keep the results secure. Pages 17 and 18 of the guidance from Weymouth and Portland Borough Council (picked because the investigation into the "Portland Spy Ring" is a good example of the sustained use of the investigatory powers of the day) illustrates why this problem is of such public concern, particularly in authorities where officials are expected to work in close co-operation with community leaders who may be more concerned with family honour than personal privacy.

33) ***Adding requirements for all those seeking to exercise powers under the Bill to provide adequate security and protection against potential abuse might well led to a welcome drop in the number of organisations seeking to retain historic powers.***

20 December 2015

Vodafone—written evidence (IPB0127)

Vodafone recognises the importance of legitimate and lawfully authorised communications surveillance in supporting the efforts of law enforcement and intelligence agencies in tackling serious crime, terrorism and threats to national security. As long as powers are exercised within a clear legal framework that is fit for purpose, workable and subject to the rule of law, few would seriously question the need for legislation that helps to maintain our nation's security, the safety of the British public and protection of the freedoms that we expect in a democratic society.

However, there is a clearly a balance that needs to be struck between protecting the UK from terrorists and criminals and ensuring that the vast majority of law abiding members of society have the right for their private information to be protected. It is for the Government to propose what powers are needed, and for Parliament to ensure that they are, and remain, proportionate. For Vodafone, trust is the bedrock of our business and our business model, which means that respect for our customers' privacy is paramount and needs to remain so.

The debate surrounding the need to update the existing legislation to ensure that the relevant authorities can get the data they need to effectively fight crime in an increasingly digital world is not new. It has spanned more than one whole Parliament and what has become clear over this period is the emergence of contradictory issues. The first is that technology and the way we communicate has changed with the wide proliferation of internet access to almost every person, home and workplace; this has fundamentally impacted the way we communicate. The second is that there remain some reservations about granting wide ranging powers to collect and retain data.

Four priorities for the Bill

We would urge the Committee to closely consider four key issues:

1. Communications data should be collected and provided to Law Enforcement Agencies by those companies best placed to do so; in particular, third party data should be retained by the provider of the service in question.
2. Proposed powers to allow equipment interference (EI) need to be carefully scrutinised and, if approved by Parliament, subjected to the most rigorous oversight regime.
3. The current oversight regime must be reformed to create a one single strong, effective and independent body. This body should be well resourced, cover all aspects of the legislation and be capable of proper liaison with other interested regulators.
4. There must be full cost recovery for communication service providers.

Our principles

We believe that greater transparency, proportionality and workability are the key factors by which this new legislation needs to be judged. Across the world, Vodafone publishes an annual Law Enforcement Disclosure Report and we operate under the following principles in regards to surveillance, namely that it should be:

- tightly targeted to achieve specific public protection aims, with powers limited to those agencies and authorities for whom lawful access to customer data is essential rather than desirable;
- proportionate in scope and defined by what is necessary to protect the public, not by what is technically possible; and
- operationally robust and effective, reflecting the fact that the internet is accessed via multiple devices – from games consoles and TVs to laptops, tablets and smartphones – and each individual can have multiple online accounts and identities.

1) Communications data acquisition and retention

We consider that there are two aspects of the proposed amendments and extensions to the regime for the retention of communications data and the powers governing its acquisition which are of particular concern:

a) The draft bill affords the Secretary of State the power to require a provider to investigate the communications carried over its network for the purpose of extracting third party communications data.
b) Public debate pertaining to Internet connection records has perhaps overlooked that the powers granted to the Secretary of State to require the retention of communications data are, in fact, far broader than just "Internet connection records".

a) Third party data

The powers within the draft Bill relating to communications data retention could be used to compel the provider of an Internet access service to obtain and retain communications data of third party "over the top" Internet communications services. Vodafone believes the responsibility to obtain and retain this data should be held by the provider of such a service – for example Facebook, Google Mail or WhatsApp – and not by the underlying network operator including Vodafone.

Network operators simply act as the "postman" for these services. If network operators were required to obtain and retain data, this would mean installing a complex new array of technology, requiring us to build systems to capture data for which we have no business purpose. We have expertise of the data which we generate in the course of running our own services for our day-to-day business activities, but we have very little knowledge, or reason to know, how any given Internet communications service or OTT service might structure its communications. The potential for this system to be ineffective, inefficient and retain too much or indeed too little data is substantial.

Any chance of this working well is much further complicated by the large scale use of encryption technologies by these internet communications providers. Where the Internet communications provider encrypts traffic to and from its servers, removal of this third party encryption is likely to be close to, if not actually, impossible from a technical perspective and, even if it were possible, the imposition of such an obligation would require an operator

to have the means to decrypt third party communications, creating a massive single point of cyber vulnerability.

We are not aware that there has been an operational justification for the inclusion of powers to require a provider to retain data relating to Internet communications services and, given the high degree of privacy intrusion and the risk associated with the technical complexity, we question whether these powers should be available to the Government at this time. Even if an operational case has been made, we consider that any duty to retain communications data should be imposed only on the provider of the service in question: the company which provides the service should retain the data.

If the Government passes legislation that means that Vodafone has to retain third party data, it should be clear on the face of the legislation that obligations can apply only to data or content affecting communications into, or within, the UK jurisdiction. It must not be possible for an obligation to require a UK operator to disclose communications data or the content of communication relating to its operations in other jurisdictions.

b) Internet connection records

Much of the public debate of the draft Bill has focused on the issue of "Internet connection records". A key problem is that these so-called "records" do not currently exist and would have to be created by piecing together information from a cross-section of different sources. Furthermore, and in our view unhelpfully, there is nothing in the draft bill about a requirement to retain Internet connection records. Rather, the wording about Internet connection records relates to requirements around authorisation for obtaining them from providers.

As drafted, the power afforded to the Secretary of State is much broader than simply obtaining internet connection records, as it states that an operator may be required to retain "relevant communications data". This is all the broader since the draft Bill expressly provides that it includes the power to require an operator to "obtain" and "generate" data.

There is nothing within the draft bill to indicate what this might mean, and could be used to require an operator to make changes to its networks and services simply to get more data — even relating to other companies' services — and to hold on to it for law enforcement.

We would welcome much greater detail and clarity on exactly what these powers will be used for, both in terms of transparency for users but also to give clarity to providers such as Vodafone what information we will or will not be required to provide. We hope that the draft bill process will ensure that greater clarity is provided before the actual Bill is laid before Parliament.

2) Equipment interference

Equipment interference is perhaps the most contentious of all the powers within the scope of the draft Bill. The obligations relating to equipment interference have the potential to

significantly undermine trust in the United Kingdom's communications service providers, and require particular attention. It clearly a matter for Parliament to debate whether these powers are proportionate but we would urge this debate to be full and comprehensive.

As communication service provider, Vodafone considers that there are three main issues:

a) The risk of diminution in trust of our services means that any equipment interference powers, if they are indeed necessary, must only be available for the most grave situations
b) Ensuring that there is no risk to the security or resiliency of our network and services
c) Ensuring that there is no involvement of a communication service provider's employees

a) The risk of diminution in trust of our services means that any equipment interference powers, if they are indeed necessary, must only be available for the gravest situations

Equipment interference amounts to a major imposition on the freedom of an operator to design and operate its services in the way it sees fit, and has the potential to breach profoundly the trust of our customers. Under the powers in this Bill, service providers could be under secret obligations to operate a backdoor in the equipment or services provided to customers. Vodafone questions whether this intrusive power is necessary at all.

If it is indeed required, any power should be legally highly constrained, and any warrant detailed and specific as to the support required and legal basis for requiring it. The situations in which such a power can be used to impose an obligation on operators, or else to attack our networks or services, must be highly constrained, and reserved for use in the most grave of situations.

In addition to the substantial risk to trust, we consider that the ability to impose equipment interference obligations will have material repercussions in the global market place for communications services, making a UK-based provider a less attractive option than a provider domiciled in a country which does not have such a framework.

b) There must be no risk to the security or resiliency of our network and services

Operators within the UK (and Europe) have obligations to ensure the security of their networks and services, and the resiliency of their networks and, more importantly, a commercial imperative to do so: it is fundamental that our services are secure and reliable to compete in the market. As such, an obligation to assist with EI must not require an operator to lessen the standard of its general security, or which could adversely impact the resiliency of its network.

This is particularly important in an environment where operators face regular attacks from third parties, and any weakening of our network or service defences, which protect critical national infrastructure and attempt to maximise the availability of essential services, would be highly undesirable.

c) Involvement of operator employees

The obligations within the draft Bill could be used to require an operator to assist not only in a passive capacity — permitting a "black box" to be installed in its network, for example — but to actively engage in the conduct of an equipment interference operation.

This would represent a significant move from a duty to provide data, or to implement an interception warrant to, say, a duty to actively seek out vulnerabilities for exploitation, or to develop vulnerabilities and exploits.

Turning network operator employees into spies and hackers is manifestly inappropriate, and the framework should be modified to expressly limit the requirement to assist to exclude this type of requirement.

3) Oversight

a) The Investigatory Powers Commission

We support the proposal to strengthen scrutiny and oversight through the Investigatory Powers Commission.
The Government is making a case for a broad range of powers to support its law enforcement and intelligence agencies in its work. Users of communications services have a legitimate expectation that their privacy will be protected, and intrusions into their privacy must be justified. The exercise of these powers must be subject to the most stringent scrutiny and oversight, to ensure that all use is necessary and proportionate.

Clearly there is a need for strong, effective and independent oversight, and we welcome the proposed creation of the Investigatory Powers Commissioner. We understand that the bulk of the oversight powers are to be given to the Investigatory Powers Commissioner, and we support the idea that there should be one oversight body with responsibility for all aspects of this legislation. This body must be adequately funded and resourced, with access to appropriate expertise.

However, at the moment, it appears that the Information Commissioner's Office, rather than the Investigatory Powers Commissioner, will be responsible for assessing some aspects of a provider's compliance. We fear that this bifurcated approach is likely to lead to a complexity and confusion, when what is needed is a simple and strong oversight regime.

We understand that the Investigatory Powers Commission is going to be responsible for the oversight of the operation and security of the request filter, and therefore it seems consistent to have the same oversight body responsible for systems which feed into it.

b) Judicial Commissioners and urgent situations

We support the idea of judicial oversight of the most intrusive powers. We recognise that, in extremely urgent situations, it may not always be possible to obtain advance judicial

approval. However, in providing for such cases, it must be clear on the face of the legislation as to the basis on which operators can be required to act, how the oversight will be ensured, and full legal protection for any operator acting under an "urgency" arrangement which is subsequently found to be non-compliant.

4) Costs of implementation

The costs, in terms of both capital expenditure (i.e. new buildings, servers, equipment etc.) and operational expenditure (i.e. ongoing costs, people etc.), associated with technical compliance with law enforcement demands, can be significant. The full cost of surveillance assistance by communication service providers should be borne by the Government as it is fulfilling the state's duty to protect citizens, and is otherwise an interference with the lawful use by a communications service provider of its assets and property. If costs are allowed to fall disproportionately on certain market players such as the network operators, this will inevitably influence the competitive dynamics of the market and ultimately the type and nature of services provided by different players.

Requiring the Government to bear the cost of surveillance both acts as a sensible restraint on the potential for excessive use of surveillance powers and also contributes to accountability by ensuring that the financial impact of surveillance is apparent, and not hidden in sunk costs borne by industry.

21 December 2015

William Waites—written evidence (IPB0089)

1. I am a researcher at the University of Edinburgh. I have also built and operated Internet and Telephone Service Providers in several countries in Europe and North America. Currently I operate an ISP called HUBS[1368] enabling service to rural and remote parts of Scotland. This response is in my personal capacity.

2. This will be a short response due to the short time that has been given to understand the bill and its implications and prepare a response. The subject matter is complex and deserves a more thorough airing. The hurry suggests a desire to stifle debate while maintaining a verneer of participativeness.

3. I note that virtually all of the responses to the public consultation of the science and technology committee expressed misgivings. The exception was the Home Secretary's response, of course. It is clear that the sentiment is against this law among those who managed to respond.

4. Mass surveillance has been rebranded as bulk. Changing the word does not change the nature of the activity. If the goal is to catch terrorists, it is provable[1369] that mass surveillance is not and cannot be effective for this purpose. Experience bears this out[1370]. No amount of legislation or wishful thinking will change that. None of bulk interception, acquisition or interference is appropriate.

5. It has been repeatedly warned that backdoors (technical capability notices, bulk interference) are as wont to be abused by criminals as they are by the good guys. This was well illustrated recently[1371] where a weakness was announced in a major vendor's firewall devices that allows passive decryption of traffic. There is no such thing as a key that only authorised people are allowed to use.

6. The burden on small providers who have not generally invested in surveillance capabilities on their network will be great. In the case of the rural providers that I work with, who are very small, requiring them to surveil their users is much more personal than requiring a large company to retain user data -- their users are their friends and neighbours. Requiring people to spy on their neighbours is particularly odious and shameful.

7. There is much overreach in the bill. The Home Office has said, for example in a meeting with the home office a colleague was assured that many of the things that could be required under the bill would not be done. "They already have retention orders with the large ISPs under the existing regime, and would expect to serve new orders only on them."[1372] What, then is the purpose of serving orders on "groups of" or "descriptions of"

[1368] https://hubs.net.uk/
[1369] https://www.schneier.com/blog/archives/2006/07/terrorists_data.html
[1370] http://techpresident.com/news/wegov/23918/denmark-government-will-not-allow-ordinary-citizens-have-digital-privacy
[1371] https://www.imperialviolet.org/2015/12/19/juniper.html
[1372] http://www.revk.uk/2015/11/home-office-ipbill.html

providers? Why are there powers in this bill that the Home Office does not intend to use? Clearly to the very great extent that this bill impinges on privacy rights the powers that we grant to the government should be the absolute minimum possible.

8. Section 46(4)(c) allow a suitably authorised officer to "ask any person whom the authorised officer believes is not in possession of the communications data but is capable of obtaining it, to obtain it..." and section 50(2) makes this a duty for the very broadly defined "telecommunications operator". This appears to create a regime where anyone who works for a company that has computers can be conscripted into an intelligence operation whether or not they have anything to do with the target/victim.

9. The operation of the bill is especially unclear because the definitions are so badly drafted. Almost anyone can be deemed to be a telecommunications operator. The definition of ``Internet Connection Record'' is not recognisable to anyone who runs a network. The most elegantly vacuous definition is the very fundamental concept of data which according to 195(1) includes "any information which is not data".

10. Were this bill to become law, and in a legal context where there is no written constitution protecting people's rights to privacy and freedom from arbitrary action by the state, it would be a very poor decision for any entity providing Internet services to be domiciled or to maintain assets in the UK. This is unavoidable for basic infrastructure providers, however the data that they can feasibly obtain is semantically poor. Application providers and equipment manufacturers -- who could be forced to provide access to semantically rich data -- are likely to simply place themselves outwith the reach of UK law.

11. There is much more to say however due to the insufficient time allowed for consulation the main points are:

    4. None of the bulk measures are appropriate or effective. They should be removed from the draft bill.
    5. The definitions are so bad as to make the law unworkable - or so much detail will have to be provided in secondary legislation that it is not possible to know what the law really means. They should be made much clearer if it is to be possible to evaluate the impact of the draft bill.
    6. Most if not all of the powers already exist in one form or another. The law in this area needs clarity and reform. This draft bill does not accomplish that and should be scrapped.

21 December 2015

Rt Hon. Sir Mark Waller—supplementary written evidence (IPB0021)

1. I was most grateful for your invitation to give oral evidence to the draft Investigatory Powers Committee on 2 December. I appreciated the opportunity to give you my perspective on the draft Bill. I write to you now because, on reflection, there are a number of areas of questioning on which either I did not make all of the points I would have liked to make, or where I was not as clear as I should have liked.

2. The first is on DV clearance for Judicial Commissioners. As I said, I would not expect the senior Judges involved to be subject to Developed Vetting partly because such Judges are accustomed in their day to day work to handling extremely sensitive material and have access to secure storage where this is necessary. But I should add that, as I emphasised during my evidence in a different context, the independence and impartiality of Judges are two of the most important characteristics of the profession. It would not be appropriate for the agencies to be involved in vetting the very Judges proposed to oversee the lawfulness of the agencies' activities and I understand that the agencies take the same view. For them to do so could be seen as giving them the ability to choose their judges and that would obviously not be appropriate.

3. The second is on training. Although I do not believe there is a need for formal "classroom" training a concerted period of on the job training is important. When I took up my post initially I spent a number of months shadowing my predecessor as well as time in the agencies learning about their systems and methods. I would advocate strongly that the new Investigatory Powers Commissioner and the other Judicial Commissioners spend a number of months shadowing the three existing Commissioners and time in the agencies getting to know how they work, their systems and their processes.

4. Finally, on the need for technical expertise, I should be clear that the answer I gave on 2 December was on the basis that the Committee were referring to whether I believed that I personally, or someone taking over my role, needed technical expertise. I do not believe they do since so much of my role is focused on the argumentation behind the request for a warrant, the necessity and proportionality and covers areas other than interception of communications or communications data. It is clear however that for the new oversight body whose remit will include the public authorities' use of communications data and interception of communications would benefit from additional technical expertise within its ranks.

5. I hope this supplementary information is helpful and I am of course available to respond to any additional questions you may have where I am in a position to do so.

14 December 2015

Daniel Walrond—written evidence (IPB0065)

1. Summary

   A. Internet Connection Records are too poorly defined. Even if they were well defined they have limited use due to poor signal-to-noise ratio and are completely disproportionate to the cost of collection.

   B. This Bill will be damaging to the security of the country, and the average citizen. It will be damaging to the economy and in an era of austerity I find it wholly unacceptable that tax payers money would be spent on this project.

   C. I have many concerns about the Draft Investigatory Powers Bill beyond what I have outlined within this submission. One of which is how avoiding detection of this Draft Bill will be trivial for technically capable people, which implies this Bill will only serve to harm innocent people and fail to achieve its objectives.

2. Introduction

   A. Having watched the video feed of the Draft Investigatory Powers Bill Select Committee on Wednesday 9th December 2015 in Committee room 2; it is quite clear there is a large gap of technical understanding between members of the Committee and some of the witnesses who gave verbal evidence. In particular; BT Security, Sky, Virgin Media, Andrews & Arnold Ltd, and ISPA.

   B. My personal background is highly technical where for my employer I have to a deep understanding of ISP level networking and will frequently interact with the same companies as an ISP would (As in tier 1 transit providers and international fibre network providers).

   C. Whilst both James Blessing of ISPA, and Adrian Kennard of Andrews & Arnold Ltd both provided the Committee with excellent verbal evidence, which was both accessible and accurate. They have only presented to the Committee a much simplified version of what is a very dense and complicated technical problem. I hope that the Committee and the Home Office will take advantage of the breadth of knowledge they hold. This is due to them having deep understanding of both the technical and business sides of running an ISP.

   D. All witnesses in the session, in my opinion, provided thoughtful and insightful evidence. Having watched their evidence, they have highlighted how controversial this Bill is; both in technical aspects and the harmful social impact this Bill will have.

3. Internet Connection Record

   A. The Internet from its conception as a Defense Advanced Research Projects Agency (DARPA) project has been built upon documents which are known as

Request For Comments (RFC). A formal process of cooperation of entities that make up the Internet. These are very important documents that allow the Internet to function. They are very dry technical documents which one must understand before implementing anything that is to function with the Internet.

B. The concept of an Internet Connection Record does not exist. Its very existence is made up by this Bill. For this Bill to be technically implemented an Internet Connection Record has to be defined to the standard of a RFC. For that to happen one must fully understand several existing RFCs. Creating an RFC is normally a lengthy process, since once defined one has to live with the unintended consequences of ill-defined protocols. Failure of taking time upfront to formally design exactly what an Internet Connection Record is before passing this Bill will lead to expensive and lengthy rewrites of software of the part of the ISPs.

C. On several occasions parallels have been drawn with Phone Connection Records and how powerful they have been at solving serious crime. From a technical stand point Phone Connection Records are very simple. There are very clear pieces of meta data of a phone call which the average person can understand. The meta data provided by a Phone Connection Record has a high signal to noise ratio. Based on the comments of several members of the Committee they have a very limited understanding of how the Internet works. Which is very understandable considering how many people I interview for technical roles who do not understand how the Internet works. Most of the focus I have seen from watching the video feed of witnesses providing evidence has been on one Internet protocol known as HTTP, focusing on just URLs. There are so many other protocols and aspects of the Internet that have not been considered where there is documented criminal activity which would not be capture by what the Committee and Home Office appear to think what an Internet Connection Record is.

D. Focusing just on the technical aspects, the amount of data the Bill is requiring ISPs to store in the form of Internet Connection Records is staggering. The specialized network equipment required to capture the data, and the data storage required is completely out of line with the turnover of a small ISP.

E. Furthermore this Bill does not just require upfront implementation costs, but will require ongoing purchases of hardware to maintain the capability. There is a very clear history of the growth of the Internet. Data capture equipment and storage will need to be purchases to keep up with this growth.

F. Even the large ISPs the costs will be harmful to their business. As for them the data storage will be a dominant cost as it will scale with the number of customers they will have. Also not just the business harm in the money required, but how it will divert skilled technical people away from more important aspects of their business. It is a serious challenge for businesses in the UK to recruit competent and skilled technical staff.

G. The average person will not realise what happens when they visit a website. This was brought up as a practical example by Adrian Kennard in that he stated he had linked to a pornhub.com image in his blog post. This is actually a very important point. No where is it visible that Adrian Kennard linked to pornhub.com on his blog post. But if you read the HTML, it is very easy to find. It is important because if this Bill is enacted then by reading his blog would lead to a persons Internet Connection Record having evidence that they have visited pornhub.com. This can be extended to anything viewable in a web browser, including hate websites, child pornography, how to make a bomb, and how to circumvent being tracked by this draft Bill.

H. As for the more innocent practicalities every web-page a person visits generates many more requests for data which will have to be recorded. This will massively add to the storage costs. Which I believe the larger ISPs will have underestimated how much an average customer will generate in terms of data to be stored as Internet Connection Records. On top of this as outlined in verbal evidence many devices that connect to the Internet will generate countless Internet Connection Records. Often these will not be generated by the direct action of the user.

I. The signal to noise ratio of Internet Connection Records will be so poor they will be meaningless. The implication of this is that much time, effort and money will be invested opening up new risks for the country.

4. Security

A. I am serious concerned if this Bill is passed on the security of Internet Connection Records. The Bill is requiring third party access to the records, this is a very dangerous part of the Bill. There's potentially highly sensitive records of people personal lives made available for many people to access. I feel this is an excessive invasion of peoples personal thoughts.

B. As a follow on, no level of oversight will protect innocent citizens of abuse. The fact that these records exist means that there will be targeted attacked on ISPs to gain access to this information, for political and blackmail reasons. It is not a question of if, but when this happens. This will be highly damaging to both the average citizen or public figures.

C. Government sponsored back-doors within encryption systems will be incredibly harmful to the security of the country, to the economy, and allow unintended interference in peoples daily lives. Once there exists a back-door, it's only a matter of time before it is public knowledge, then used against both the nation and state.

5. Technical Abuse

A. ISPs have provided estimated costs of implementing the Bill. I do not think they

have considered the level of abuse they may be subject to. It will be trivial for ISPs to be subjected to denial of service. Or at least very costly storage problems. Due to the requirement for the ISPs to storage every so called Internet Connection Record, it will not be hard to abuse this and generate very high volume of fake records that will be disproportionately expensive to store.

B. Depending upon implementation it will probably not be hard to fake connection record to incriminated other people. My expectation is that to reduce the probability of this type of abuse will further increase the costs of implementation.

C. Both of these types of abuse will make the already low value of recording Internet Connection Records even lower.

20 December 2015

Rev Cecil Ward—written evidence (IPB0013)

1. I feel that the progress of the Draft Investigatory Power bill should be halted until certain conditions are met, and there should be an immediate statement that it is "on hold".

2. The first condition is that an independent expert body should _clarify_ the terms "internet connection record" and "communications data" completely, at a fully adequate technical level. In particular, appeals to leave these terms vague on the grounds of future-proofing are not acceptable.

3. The second condition is that the sections permitting "equipment interference" should be removed. If needed, this topic should be addressed in a separate proposal to be put before parliament, and this would have to be (i) clear, free of weasel words and (ii) where hacking is recommended it should use the word "hack" or "breaking in", (iii) where the introduction of malware is recommended it should say so and explain in detail what malware is, and (iv) point out what damage is inflicted and what changes are made to machines or software systems concerned.

4. A published explanation of the exact limits on the range of demands that may be imposed on small ISPs and large ISPs should be published so that Parliament and see the extent of onerous and worrying possible effects on the relationship between (especially) small ISPs and their customers, the effect on their businesses, and the effect of on British business as a whole and its competitiveness internationally. Parliament should have the opportunity to discuss such a clarifying document.

5. This document represents my concerns about the urgent need for clarification (i) especially at a technical level, where vague terms are used because non-technical authors have used everyday language assuming that it is appropriate and assuming an imagined model of how the Internet, devices, software systems, applications and services work that is not remotely adequate or meaningful to technical people with a correct (not imagined) understanding, and (ii) clarification about exactly what demands may be placed on ISPs, especially small ISPs, using precise technical language (and also explained fully in everyday English for non-technical readers), and (iii) with the detail expounded in p. 2.ii having the happy effect that it constrains future Home Secretaries. I have other concerns but they are not addressed here.

6. The entire bill is a cause for concern, not an offer of improvements to our way of life. (Why is this? How does raising great alarm amongst the informed section of the public constitute progress or an achievement on the part of the proposers of the draft bill?)

7. This opinion, which I claim is uncontroversial, commonly held wisdom, absolutely requires that extremely great diligence and skepticism be exercised before proceeding, and unless it is shown to be the case that the freedoms that we currently enjoy are demonstrably protected, common wisdom absolutely requires

that the progress of the bill be halted without fear of having participated in failure in any way.

13 December 2015

David Wells—written evidence (IPB0166)

1. My name is David Wells. I was a GCHQ intelligence officer from 2005 until 2013, and worked for a partner intelligence agency in Australia until late 2014. Although I no longer work in the classified intelligence environment, I have significant and contemporary experience working with bulk communications data, particularly in the Counter-Terrorism (CT) environment.

2. I am providing this evidence in a personal capacity at the suggestion of the Head of the Joint Committee's Secretariat. This request came in response to a blog post in which I addressed some of the arguments presented to the Joint Committee by Mr William Binney, a retired technical director of the NSA.

3. Mr Binney's evidence did not correspond with my own, more recent experience. Specifically, I disagreed with his claims that there was 'no good operational case for bulk interception', and that in CT, this approach resulted in 'lives being lost'.

4. I am subject to the restrictions of the *Official Secrets Act 1989*. As such, I intend to provide a high-level overview of the utility of bulk communications data in intelligence and CT, based on my experience.

5. To do so, I would first recommend that the Committee re-consider the needle/haystack analogy typically used when discussing intelligence agency use of bulk datasets. Instead, consider how you and millions of others use the Google search engine, and how much Google – like the ability of intelligence agencies to process big data - has changed over the past 15 years. *(I use this analogy to more accurately reflect changes in the use of big data, not to suggest Google and UK intelligence agencies have access to similar data volumes or types of data.)*

6. Initially, Google only allowed relatively simple search terms. Many businesses had little or no internet presence, while Google's 'web-crawling' technology did not necessarily access all those that did. In short, it lacked a comprehensive dataset to query, and as a result, it was difficult to use with confidence.

7. These data inconsistencies meant that you could not be certain that Google had access to the data you were looking for, or whether the results it pulled back were relevant to your initial query. Like the intelligence analyst described by Mr Binney, you were confronted by too much irrelevant data. Even after clicking through multiple pages of results, you might not find what you were looking for; an alternative, more targeted method (say a local phone book) was often more effective.

8. In 2016 however, 'big data' is a reality. The internet is growing exponentially and plays a central role in everyday life. As a result, the Google search engine has access to a comprehensive and growing dataset. It is in the business of 'bulk collection'.

9. This does not mean that as an individual user, you are overwhelmed by data. Instead, the increase in data volume has been accompanied by the ability to ask complex and nuanced questions. This reduces the number of results your query brings back, but also increases

their relevance. In most instances, you get the answer you're looking for on the first page, if not in the top result.

10. Similarly, while intelligence agencies in the UK and elsewhere have access to more communications data than ever before, by using focused queries and data filters, intelligence analysts only need to retrieve and analyse a small fraction of the overall dataset. As with Google, having more data improves the quality of your results. Intelligence analysts can get the data they need comparatively quickly and efficiently.

11. Mr Binney's evidence further suggested that the UK intelligence agencies (and the Joint Committee) could make a choice between bulk data collection or targeted technical surveillance. The former, '99% useless and putting lives at risk'; the latter 'operationally effective and reducing the privacy burden'. This is not the case.

12. Returning to the analogy, people typically use Google to discover new information, or to remind themselves of information that they have forgotten or misplaced. Simultaneously, they will also use a number of websites or apps on a regular basis for a 'targeted' service – you access Facebook or the BBC website because it gives you the information you already know you want.

13. Similarly, analysis of bulk communications data and focused data collection on 'targets of interest' serve different but complementary purposes. Intelligence agencies cannot exclusively focus on the latter group; they also need to discover new targets and 're-acquire' targets they have lost access to. Like Google and 'favourite' websites, bulk data and targeted collection answer different questions in a different but mutually beneficial way. It is not a question of either/or.

14. The suggestion that UK intelligence agencies work outwards from known targets *instead* of using bulk collection is therefore based on one of two incorrect assumptions: either all the individuals that intelligence agencies require access to have already been identified; or those currently unknown (or subsequently unknown) can all be discovered through analysis of known targets. Unfortunately, the world of intelligence is not that static or predictable.

15. In the context of the Committee's review of the IP Bill then, it is not a question of making a high-level choice between different intelligence collection strategies. Rather, how does the UK best balance these sources and approaches from a resourcing and prioritisation perspective? What works best for the intelligence problems we face now and will face in the future? These questions do not have simple answers, hence the range of powers and proposals contained in the Bill before you.

16. I am not authorised to provide you with specific examples of how and when different types of data are used by intelligence agencies. I hope however that my submission demonstrates that - contrary to some of the evidence provided to the Committee - bulk communications data does and should play a critical role in the work of UK intelligence agencies.

20 January 2016

Peter White—written evidence (DIP0004)

I am writing to express my concerns about the draft Investigatory Powers Bill. My view is that the powers requested are excessive, unnecessary and unworkable.

It is clear that there is a need for clear, well-drafted legislation to codify the powers of the police and security service and establish oversight. However, the rights proposed in this document are wildly excessive. In particular, they allow the security services (and for that matter a whole range of other government bodies) to collect a vast array of data without either a justification or any oversight (in particular, the judicial oversight appears only to ensure that the rules are followed, not that any given target of surveillance is appropriate, something that would, for example, allow the collection of information about people for political reasons).

Interestingly, the justification for these powers is often claimed to be the struggle against terrorism. However, in almost every case of recent terrorism these powers would not have helped; almost invariably the perpetrators were known to the authorities who either did not have the resources to investigate, or else failed to share information effectively thanks to process issues that this bill does not address. There are clear issues there, but throwing more data into a system that cannot handle the data it has does not seem particularly helpful.

Finally, there are issues regarding the impact of this legislation on the UK's software and communications infrastructure. Apart from the incredible requirements for secrecy, and the level of penalties for giving away information about security, there is the question of the cost of having to monitor and record all IP addresses access from every computer, correlate those with the associated DNS name, and figure out what that implies in terms of human access to services such as social media. It's not clear if it is possible for the ISPs to keep enough information to be of any use at all and it is clear that it will be expensive and difficult for them to do. A couple of popular technical press articles on this are linked to below, for example.
http://arstechnica.co.uk/tech-policy/2015/11/the-snoopers-charter-would-devastate-computer-security-research-in-the-uk/
http://arstechnica.co.uk/tech-policy/2015/11/uk-isp-boss-points-out-massive-technical-flaws-in-investigatory-powers-bill/

The net of this is that this is a bill which is so ill-conceived and poorly thought through that it will have negligible impact on national security; will lead inevitably to abuses by the "security services" (in the loose sense of the organisations listed under RIPA); and will have a serious detrimental impact on the UK software industry and internet infrastructure. It's hard to see how such a poor bill can be transformed into anything fit for purpose.

5 December 2015

Adrian Wilkins—written evidence (DIP0003)

My qualifications

I have made my living in the IT sector for the last 17 years since leaving the medical profession. I have experience of, and an interest in, encryption systems and the privacy of personal data (through my work in the healthcare IT sector).

Are the powers sought necessary?

I don't believe a case has been made.

Take note that these are powers that are being exercised in secret anyway. The legislation merely seeks to make them legal ex-post-facto (and expand them).

Yet these powers did not manage to prevent the Paris atrocities - despite them being coordinated using ordinary, plain text, SMS messages, easily intercepted.

The intelligence community itself must surely be aware that the powers being sought can be avoided with the most basic of age-old tradecraft. Bin Laden's followers knew never to use the phone, would communicate with him through couriers, etc.

Are the powers sought workable?

I believe they are not just unworkable, but counterproductive.

Unworkable

The banning of encryption as a service that cannot be circumvented by the service point will simultaneously have ill effects on the confidence in much of existing internet infrastructure, and have no effect on those well-informed people who seek to use encrypted communications for malign purposes.

- Military grade encryption technology is, and has been, available to the general public for decades.
- It is not dependent on provision by a service provider - anyone with a computer can construct an independent encryption capability resistant to attack by even the most determined and resourceful opponent.

Meanwhile, much of the network infrastructure of the world now depends on strong encryption that cannot be compromised easily. Mandating that mechanisms to compromise these communications be built into existing systems is not just foolish, but given the international nature of network communications, pointless - you will inevitably have to communicate with an endpoint that has no such foolish restrictions.

I have already seen examples of companies that have been put off setting up operations in the UK, just as a result of the proposed legislation.

Counterproductive

Let us suppose that someone invents a 99.99% accurate terrorism detection algorithm. Let us then feed it the digital traffic of the population of the UK.

99.99% accuracy means that 1 in every 10,000 times, it will falsely identify an innocent person as a potential terrorist.

In a population the size of the UK, this means that you will then have 6,500 new terrorism suspects that you must vet to ensure that they mean no ill will.

- This is incredibly expensive, requiring the attention of skilled case officers
- If any in-person interviews are required, this will amplify suspicion and discontent amongst targeted groups
- This ties up case officers doing a vast amount of work that is known, beforehand, to be of no significant intelligence value

And this ignores the fact that a 99.99% accuracy level is ridiculously optimistic. 99.9% accuracy? 65,000 suspects. 99% accuracy? 650,000 suspects.

Blanket surveillance is therefore clearly unworkable as a means of detecting terrorists. The logical thing to do would be to expand human intelligence operations, as these can be far more specific and targeted.

Are the powers sought sufficiently supervised?

The immense power of computer systems to manipulate and move data around is difficult to comprehend for many.

For example, take the incident where a gentleman received coupons from his supermarket for baby products. He thought this was a mistake - until his daughter, a holder of a duplicate of his store card, confessed that she was pregnant. The supermarket had managed to infer, from her buying habits (a cessation of the purchase of alcohol and feminine hygiene products), that she was expecting a baby and roughly when.

By default, computers make data easy to access. To make a system that is difficult to access, that requires checks and balances, is far harder than that default position. By creating such a vast capacity to observe the habits and behavior of the citizens of the UK, you create a tempting and valuable target for all those who would misuse that capacity.

Since, as observed above, it serves no purpose as a terrorism detector, you might conclude that the creation of this capacity is the reason for the bill. The power that this capacity would grant is both awe inspiring and frightening and must be guarded against. There are NO safeguards sufficient to guard against the misuse of these powers once they are created, because they will either (as we have seen) be used anyway, in secret, or legislation will be passed to make their use legal. The only way to protect against the unwarranted acquisition of this power is to prevent its creation in the first place.

Adrian Wilkins—written evidence (DIP0003)

4 December 2015

Professor Andrew Woods—written evidence (IPB0114)

Written evidence submitted by Professor Andrew Keane Woods

Introduction

1. I am pleased to submit this written testimony regarding the Draft Investigatory Powers Bill. I am an assistant professor at the University of Kentucky College of Law. My scholarship focuses on jurisdictional and conflicts-of-laws issues related to the Internet. I have written extensively about cross-border law enforcement requests for mutual legal assistance in order to obtain foreign-held or foreign-managed data, including a report for the Global Network Initiative regarding the urgent need for reforms to the mutual legal assistance regime.

2. My main concern with the Bill is its extraterritorial reach. Specifically, I worry about how the Bill interacts with the mutual legal assistance regime as it applies to cross-border requests for data in two contexts: (1) U.K. government requests for MLA regarding overseas-held data; and (2) foreign government requests for MLA regarding U.K.-held data. Furthermore, I think the Bill could better articulate the high-level principles that should inform future international agreements regarding government access to foreign-held data.

U.K. Government Requests for Overseas-Held Data

3. The Draft Bill explicitly applies extraterritorially. Because so many Britons use Internet services that are managed abroad, the Bill could have significant implications for overseas service providers.

4. For example, a great deal of the evidence that British law enforcement agents seek is controlled by American technology firms. Under existing U.S. law, an American provider may only produce domestically-held data in response to a warrant from an American judge. This means that if British law enforcement agents seek data held in the U.S., they must ask the U.S. government for assistance under the countries' bilateral MLA agreement.

5. While the Bill appears to suggest that American law makes it not "reasonably practical" for a U.S. provider to comply with a British warrant for U.S.-held data, it is not entirely clear. The Bill could clarify this important point.

6. Just as importantly, since a great deal of requests for foreign-held data will likely be made via MLA – by my estimate, the number of requests could reach tens of thousands of requests per year – the Bill should articulate standards for the British government's handling of MLA requests.

7. Specifically, I would suggest that the Bill be revised to require four things:
    a. Training for law enforcement agents seeking foreign-held data in connection with an investigation;

b. Developing and disseminating a standard MLA request tool;
c. A centralized digital tracking system for MLA requests; and
d. A transparency report, to be published every year by the Investigatory Powers Commission (IPC), regarding the number and types of cross-border data requests made by the British government.

Foreign Government Requests for MLA Regarding U.K.-held Data

8. Foreign governments often find themselves in the same situation as the U.K. government – seeking data that is held beyond their borders. When the data is held in the U.K., the government seeking the data must request MLA from the British government. The U.K. intake procedures therefore must be improved.

9. This could be achieved through a number of measures, including:
   a. Better coordination with foreign partners;
   b. Developing a centralized digital tracking system for MLA requests; and
   c. Tasking the IPC or a similar body with special instructions for handling MLA requests related to Internet data.

International Agreement Regarding Cross-Jurisdictional Data Requests

10. Finally, and more fundamentally, since the MLA regime will in my view be unable to manage the number of requests between the British government and foreign Internet service providers for evidence, I would also encourage the development of a new international agreement articulating the scope of the government's authority regarding Internet data managed by a foreign company.

11. The goal of such an agreement should be twofold: (1) to maximize user privacy, while (2) ensuring that British law enforcement have expedited access to overseas data in those cases where it is legitimately needed.

12. Such an agreement would of course be struck independently of the Investigatory Powers Bill, but as a flagship piece of legislation that seeks to articulate the British position on government access to data, the Bill could nonetheless articulate several principles that should guide British diplomacy in this area. For example, the Bill could clarify that any cross-border data sharing arrangements must meet a number of strict due process requirements – such as particularity, legality, severity, notice, and minimization requirements, among others – as well as accountability and oversight measures.

13. To that end, in line with the recommendations above, the Bill should also require that the IPC publish an annual report with detailed information on the number of requests that the British government makes to foreign governments regarding data and the number of requests that it receives.

21 December 2015

Professor Lorna Woods—written evidence (IPB0163)

1. I am a professor in the Law School at the University of Essex and a solicitor formerly in practice in London. My former practice areas and my research interests lie in the fields of information and communication industries, including the media and the Internet.
2. This submission is made in my personal capacity and the views expressed should not be attributed to my employer.

Introduction

3. I was invited to lead an ad hoc working group on the draft Investigatory Powers Bill (IPB). The objective was to produce a clause-by-clause review of the IPB. We aimed to identify where a provision was new, or where it was a reiteration of an existing provision. We sought to cover not only statutory sources, but also the relevant codes of practice (where published) and the three reviews carried out by the ISC, David Anderson QC and RUSI. The resulting review is annexed to this submission.

4. We have taken the view that the clauses fell into one of three categories:
    a. The same as or functionally equivalent to a pre-existing provision;
    b. Completely new; or
    c. Amended/extended.

    Where the IPB introduces a specific regime to deal with a practice that was carried out under a general power, such as s. 5 Intelligence Services Act, we have treated that regime as new. This approach appears to match that of the Joint Committee in its Call for Evidence.

5. Although our primary objective related to the identification of relevant sources, we also indicated the significance of the changes as well as issues where we were not sure of the consequences of the drafting/changes identified. The aim of this project was not to provide a detailed analysis of the entire IPB but rather to provide a tool to assist others in any such undertaking. Further, given the time constraints under which we operated, it is clear that there is more detail from the various sources, as well as more comments on the substance, that could be included. Another consequence of the speed with which the documents were prepared is that they are not as heavily edited as one might normally expect and there is a lack of a single authorial voice. This does not affect the validity of the content.

6. The members of the ad-hoc group included: Andrew Cormack, Ray Corrigan, Julian Huppert, Nora Ni Loideain, Marion Oswald, Javier Ruiz Diaz, Graham Smith, Judith Townend, Caroline Wilson Palow, Ian Walden. The contributors came from a range of backgrounds but all contributed in their personal capacity. A wider group of academics and practitioners were involved in discussions over email and at two meetings held at the Institute of Advanced Legal Studies in autumn 2015. Some have given individual evidence to the Select Committee.

7. I would like to highlight a number of issues based on the content of the review, as well as my own knowledge and experience.

Overarching/thematic Questions

Are the powers necessary?

8. It is less easy to claim that a broad range of highly intrusive powers are necessary by comparison to a narrower range of powers that are more targeted in their focus. The review shows the extent to which the IPB introduces new powers or powers of an extended scope which range from the targeted (such as content interception) to the indiscriminate (e.g. bulk equipment interference as can be seen in relation to Parts 5 and 6). While the provisions on equipment interference and bulk personal datasets clearly represent an expansion of powers (or recognition of existing behaviours), there is a trend towards the expansion of powers that is less immediately apparent.

9. This expansion arises in two ways in particular: changes to definition and normalisation of techniques.
    a. Changes to definitions: The wording of a particular provision may be broadly similar to or even replicate that in the Regulation of Investigatory Powers Act (RIPA), but the scope of the power will change if the definitions of the words used alter. There have been numerous changes of this nature, most if not all, operating to expand the scope of the definition. Examples include 'telecommunications operator', 'communications data' (see comment on cl. 193), 'apparatus' (see comment on cl. 195), and 'interception' (see comment on cl. 3).
    b. Normalisation of techniques: Supporting measures such as capability maintenance, which include broad ranging obligations on operators, which in RIPA were linked to interception warrants seem now to be applicable to most powers (see comment on cl. 189). National security notices likewise seem to apply broadly.

Are the powers legal?

10. It is difficult to say in abstract whether the powers themselves would be legal, because much depends on the particular power, the detail to be provided in the Codes and how the process operates in practice. Beyond that, the legal landscape in both the EU and the ECHR as regards Article 8 European Convention on Human Rights (ECHR) and Article 7 European Charter of Fundamental Rights (EUCFR) is in a process of development, with decisions such as *Zakharov v. Russia* (Grand Chamber),[1373] *Szabo and Vissy* v. *Hungary*[1374] emanating from the European Court of Human Rights (ECtHR) and, from the Court of Justice, *Schrems*[1375] (Grand Chamber) and *Digital Rights Ireland*[1376] (Grand Chamber). While the ECtHR and the Court of Justice refer to one another's decisions, it is less clear whether they take exactly the same line. The Court of Justice has taken a strong stance against mass surveillance,

[1373] Application no 47413/06, judgment 4th December 2015
[1374] Application no 37138/14, judgment 12th January 2016
[1375] Case C-362/14, judgment 6th October 2015
[1376] Joined Cases C-293 and 294/12, judgment 8th April 2014

whereas the ECtHR – at least in *Szabo and Vissy* –seems to be more accepting of its necessity (para 68). The same court, however, referring to the Court of Justice in *Digital Rights Ireland*, also highlighted the need for higher standards of protection than previously (para 70).

11. The ECtHR's case law requires the law to be foreseeable. Beyond the still complex drafting of the IPB, there are questions about whether the activities which may trigger surveillance as well as the identification of the groups the subject of surveillance.
    a. The grounds on which a warrant may be deemed necessary are broadly drafted, using terms such as 'national security'. While the IPB states that the case for the necessity of the warrant must not just restate such phrases, it accepts that general justifications may be given. It is questionable whether this requirement meets standards that may be extrapolated from the ECtHR in *Zakharov*. There, the ECtHR criticised the breadth of discretion granted to the executive in cases dealing with national, military, economic and ecological security (para. 247-8).
    b. Despite concerns raised in the reviews, the IPB provides for thematic warrants (see comments related to cl 13 and cl. 83). In *Zakharov* the ECtHR was critical of the Russian system in that it allowed interception that was not linked to specific persons but rather targeted an area (para 265). The concern was re-iterated in *Szabo and Vissy* that the authority to identify the subjects of interception 'either by name or as a range of persons' 'might include indeed any person and be interpreted as paving the way for the unlimited surveillance of a large number of citizens' (para 66-67).

12. The IPB standardises many aspects of procedure and oversight with regards to the various powers. While this may create a more easily understood structure, it may not award sufficient oversight to the most intrusive forms of surveillance, which in turn affects the acceptability of the system under Article 8(2) ECHR. Consider the potential intrusiveness of the use of bulk personal data sets, or of equipment interference as the Internet of Things becomes more established. This standardisation has also had the unfortunate side effect that pre-existing bulk interception warrants are extended from the current 3 months to 6 months.

13. The ECtHR in *Szabo and Vissy* emphasised the need for the law to protect journalists' sources by requiring judicial approval in advance, as well as other sensitive professions (para 77). This would seem to apply to content as well as communications data. The IPB does not give strong protection in this regard (see comments on cl. 61).

Are the powers well delineated?

14. Some of the definitions are very broad and open-ended. This seems to be an attempt to draft in technologically neutral terms. The definitions may lead to problems from a technical point of view but even just from a textual perspective it results in difficulties understanding what lies within the scope of the power, and what lies outside. An example of this problem can be seen in relation to the ability

to collect communications data acquired as a result of bulk interception (see comments related to cl. 106). There are also difficulties in maintaining the distinction between the 'content of a communication' and 'communications data', which runs through the entire bill (see e.g. cl. 3, 12, 16, 33, 45, 106, 119, 121 as well as in the definitions section, 193). The relationship of different forms of data is not clear, and nor is the outer extent of the term. This may lead to competence creep, especially as technology changes (see also comments cl 149/136 in relation to 'equipment'; scope of cl. 71). Conversely, there are some terms that are not defined, for example in cl. 47 the term 'internet communications service', which may lead to uncertainty.

Are the powers sufficiently supervised?

15. One of the important aspects of the IPB is the introduction of oversight mechanisms (via the Judicial Commissioner process and the 'double lock' mechanism, and the consolidation of various external review bodies into a new body, the IPC). This is significant in terms accountability and control, especially given the breadth of the powers in the IPB. Yet there are questions as to the standard of judicial review to be applied (see e.g. comments on cl. 19) and whether review, as opposed to authorisation, is sufficient. These questions have become increasingly important in the light of Grand Chamber judgments from both European courts regarding mass surveillance and technical bypassing of oversight procedures. In *Zakharov*, the ECtHR was particularly critical of the application of formal criteria, rather than the real verification of both the necessity and proportionality of the measures (para 263). Similarly in *Szarbo and Vissy*, the safeguard that national security powers could be used only when the relevant information could not be obtained any other way was not, on its own, sufficient. The ECtHR noted that there was no legal requirement to produce supporting evidence by which reviewing authorities could actually assess assertions of necessity (paras 70-72). *Zakharov* also emphasised the importance of ongoing scrutiny (see comments on cl. 170).

16. The ECtHR in *Zakharov* accepted the possibility of emergency measures, but it determined that there were insufficient safeguards about the possibility of abuse (para 266; see also *Szarbo and Vissy*, paras 80-81). In the IPB, unjustified use of emergency powers must stop only in so far as 'reasonably practicable' and 'as soon as possible' (see cl. 21 IPB and analogous provisions). Moreover material thereby intercepted may still be used (with the approval of the judicial commissioner). It is arguable that this undermines safeguards against unnecessary use of emergency procedures.

17. Part 8 contains the oversight arrangements. The extension of oversight arrangements to powers which had been exercised under general provisions, such as s. 5 Intelligence Services Act, is an improvement. Yet, as the comments to that part indicate, there are also questions about the independence of the IPC (see comments on cl. 167 -169), the scope of his/her review functions, and regarding the operation of the new error reporting provisions (see comments on cl. 171). Given the importance of safeguards and oversight mechanisms for a finding of legality under Article 8 ECHR, these provisions require further attention.

Part 1 Investigatory Powers Draft Bill - Review of drafting provenance – Investigatory Powers Research Group. This working document may be subject to change, following further assessment. For abbreviations and full source list go to bit.ly/ipbillsources. Comments/suggestions to: ipbillresearchgroup@gmail.com.

IPB reference	Description of content	IPB extract	Source	Description in legislation / reviews	Issues/comments
1	Overview				Presumably this is an attempt to write in non-technical language suggested by Anderson Rec. 3 Does statement actually match up with reality? Does it reaffirm 'the privacy of communications' Anderson Rec 1(a).
2(1)	Re-worded re-iteration of offence in RIPA	A person commits an offence if (a) the person intentionally intercepts any communication in the course of its transmission by means of (i) a public telecommunications system; (ii) a private telecommunication system (iii) a public postal service	RIPA, s 1(1) and s. 1(2)	It shall be an offence for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of (a) a public postal service; or (b) a public telecommunications service Note ISC Rec. T	The reference to 'lawful authority' contained RIPA is found in IPB s. 2(1) (c) and the reference to 'in the United Kingdom' rom RIPA is found in IPB s. 2(1)(b). Cl. 2(1)(a)(ii) reflects RIPA s. 1(2) While the wording is the same, the provision's scope will have changed due to changes in definitions. See also Explanatory Memorandum.

2(2)	Consent of owner of private system to interception	But it is not an offence under subsection (1) for a person to intercept a communication in the course of its transmission by means of a private telecommunication system if the person…	RIPA s. 1(6) and 1(3)	The circumstances in which a person makes an interception of a communication in the course of its transmission by means of a private telecommunications system are such that his conduct is excluded from criminal liability under subsection (2)…	IPB refers to cl. 2(1) *in toto* but because of the limitation in cl. 2(2) to 'private telecommunications system', effectively this covers just 1(a)(ii) thus matching the scope of RIPA 1(6) (save for changes in scope due to definitions) The right of action under s. 1(3) RIPA has gone.
2(3) - (5)	Cross-reference to definitions in sections 3-5, and sections 193-4				
2(6) - (7)	Offence under ss(2)(1)	A person who is guilty of an offence under subsection (1) is liable - (a) on summary conviction in England and Wales, to a fine; (b) on summary conviction in Scotland or Northern Ireland, to a fine not exceeding the statutory maximum; (c) on conviction on indictment, to imprisonment for a term not exceeding 2 years or to a fine or to both	s. 1(7) RIPA		NB difference in respect of Scotland and NI.
2(7)	Requirement for consent of DPP for prosecution		s. 1(8) RIPA		

3(1)	Defines the act of interception in relation to a telecommunications system	For the purposes of this Act, a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if,- (a) the person does a relevant act in relation to the system, and (b) the effect of the relevant act is to make some or all of the content of the communication available at a relevant time to a person who is not the sender of intended recipient of the communication.	s. 2(2) RIPA	For the purposes of this Act, but subject to the following provisions of this section, a person intercepts a communication in the course of its transmission by means of a telecommunications system if, and only if, he- (a) so modifies or interferes with the system, or its operation, (b) so monitors transmissions made by means of the system, or (c) so monitors transmission made by wireless telegraphy to or from apparatus comprised in the system, as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication.	Definition of telecommunications system is found in cl. 193; note comments on extension of scope in relation to that clause. Transmission – found in s. 2(2) RIPA – is dealt with at cl. 3(4) IPB (see below).
3(2)	'Relevant act'	In this section "relevant act", in relation to a telecommunication system, means - (a) modifying, or interfering with, the system or its operation; (b) monitoring transmissions made by means of the system; (c) monitoring transmissions made by wireless	s. 2(2) RIPA	See above	Rephrases s. 2(2) RIPA. 'Apparatus' defined cl. 195(1) in what may be broader terms. See comment in respect of cl 195(1).

		telegraphy to or from apparatus that is part of the system.			
3(3)	Modification of a telecommunications system		s.(2)6 RIPA		While phrased in similar terms to s. 2(6) RIPA, note impact of changes to definition of 'telecommunication system'.
3(4)	Extension of 'time when in course of transmission' definition	'any time when the communication is stored in or by the system (whether before or after its transmission)' 3(4)(b)	RIPA	Any time when the system by means of which the communication is being, or has been, transmitted is used for storing it in a manner that enables the intended recipient to collect it or otherwise to have access to it 2(7)	More extensive than RIPA. It seems that 'sent' items and those in draft folders might be covered in interception. See Explanatory Memorandum for further examples. NB: re-worded formulation again. It clarifies the remaining uncertainty over RIPA, s. 2(7), following *Edmondson & ors v R* [2013] EWCA Crim 1026.
3(5)	When is content available	is taken to be made available to a person at a relevant time include…'	s. 2(8) RIPA	are taken to be made available to a person while being transmitted shall include…'	Follows through on extension to ss.3(4) by inclusion of (b).
3(5)	Recorded conversations		s. 2 (8) RIPA		No change, but presumably applies within the context of broader definition of communications system and note definition of content of communication at cl 193(6),

					and notes accompanying that provision.
3(6)	Definitions for interference with wireless telegraphy		ss. 115 - 177 Wireless Telegraphy Act 2006		
3(7)	Interception in re postal services in transmission	section 125(3) of the Postal Services Act 2000 applies			
3(8)	Interception in the UK		s 2(4) RIPA		
					Structure different - relevant definitions found in s. 3(2) and 3(4) IPB. Note deletion of 'while being transmitted' and note comments re ss 3(4). Interception is understood in wider terms because of the changes to cl 3.
4(1)	Receiving broadcasting is not interception		s.2(3) RIPA		No change.
4(2)	Using 'postal data'	References in this Act to the interception of a communication in the courts of its transmission by means of a postal service do not include references to…'	s. 2(5) RIPA	References in this Act to the interception of a communication in the course of its transmission by means of a postal service or telecommunications system do not include….'	RIPA refers to 'traffic data' (defined s. 2(9), (10) and (11) RIPA); IPB excludes telecommunications system and refers to 'postal data'

					(defined s 194, see comments).
5	'Lawful authority'	.. A person has lawful authority to carry out an interception if, and only if…'	s3 RIPA		Different phraseology - RIPA refers to the subsection authorising conduct; the list of lawful conduct is different. NB under IPB conduct lawful under s. 5 is to be lawful for all purposes.
7	Requests for interception to overseas authorities	The Secretary of State must ensure that no request to which this section applies is made on behalf of a person in the United Kingdom to the competent authorities of a country or territory outside the United Kingdom unless a mutual assistance warrant has been issued	See Anderson Rec. 8, 76-78	Receipt/transfer of intercepted material should be subject to clearly defined safeguards	Applies to EU mutual assistance warrants or action under an international mutual assistance agreement. See further Part 2.
8	Offence of obtaining communications data	A relevant person who knowingly or recklessly obtains communications data from a telecommunications operator or postal operator without lawful authority is guilty of an offence.			This is new. According to the Explanatory Memorandum, it is to act as a deterrent. Offence only applies to 'relevant person' - that is someone within a 'relevant public authority' within the meaning of Part 3 IPB. Part 3

					then takes you to Schedule 4 which lists authorities. Note ability of Secretary of State to amend schedules. Mens Rea is easier to satisfy than for s. 2 offence.
9	abolition of 'general information powers'	(2) Any general information power which- (a) would (apart from this subsection) enable a public authority to secure the disclosure … of communications data … is to be read as not enabling the public authority to secure such a disclosure		Anderson Report recommended that existing legislation should be replaced by single framework - see Rec. 1, 6 & 7. See list in Annex 6.	ss. (1) cross refers to Sch 2. Note power of SoS to modify 'any enactment in consequence of subsection (2)'. 'General information power' is defined at s. (9)(5). Note there is no complete repeal; there are other parts of the bill where existing statute remains too. This provision brings the Code of Practice obligation (at 1.3) into the statute.
10	Circumstances in which 'relevant services' may hack	..may not.. Engage in conduct that could be authorised by a targeted interference warrant or a bulk equipment interference warrant except under the authority of such a warrant if- (a) … the conduct would..constitute one or more offences under sections 1 to 3A of the Computer Misuse Act 1990... and (b) there is a British Islands connection'	Anderson Report Rec 6(b)	"The following should be brought into the new law and/or made subject to equivalent conditions to those recommended here …. (b) equipment interference (or CNE) pursuant to ISA 1994 ss 5 and 7, so far as it is conducted for the purpose of obtaining electronic communications..."	The provision aims to exclude reliance on ISA when it falls within the subject matter of the IPB. The application of the IPB is subject to 2 conditions: existence of an offence under Computer Misuse Act (ss 1-3A), which are broadly defined; and a connection to the British Islands (defined ss(2)). Absent

					both conditions, a warrant is not required. There is no offence for misuse.
11	Restriction on use of s. 93 Police Act	A person may not, for the purpose of facilitating the obtaining of communications, information or equipment data, make an application under section 93 of the Police Act 1997 for authorisation to engage in conduct that could be authorised by a targeted equipment interference warrant if the applicant considers that the conduct would (unless done under lawful authority) constitute one or more offences under sections 1 to 3A of the Computer Misuse Act		Note Anderson Report, Rec 2: changes required to Part III Police Act (s. 93 authorisations to interfere with property).	This seeks to ensure that the provisions on equipment interference are not circumvented by reliance on the Police Act.

Part 2 Investigatory Powers Draft Bill - Review of drafting provenance – Investigatory Powers Research Group. This working document may be subject to change, following further assessment. For abbreviations and full source list go to bit.ly/ipbillsources. Comments/suggestions to: ipbillresearchgroup@gmail.com.

IPB reference	Description of content	IPB extract	Source	Description in legislation / reviews	Issues/comments
12(1)	Establishes three types of warrant	There are three kinds of warrant that may be issued under this Chapter: (a) targeted interception warrants (see subsection (2)), (b) targeted examination warrants (see subsection (3)), and (c) mutual assistance warrants (see subsection (4))	see below	ISC Report, Rec B	Interception defined in cl. 3. Note impact of changes in definition on scope.
12(2)	Creates targeted interception warrants	A targeted interception warrant is a warrant which authorizes or requires the person to whom it is address to secure … any one of the following- (a) the interception, in the course of their transmission by means of a postal service or telecommunications system, of the communications described in the warrant; (b) the obtaining of related communications data from	largely RIPA 5(1)	(1) Subject to the following provisions of this Chapter, the Secretary of State may issue a warrant authorising or requiring the person to whom it is addressed, by any such conduct as may be described in the warrant, to secure any one or more of the following— (a)the interception in the course of their transmission by means of a postal service or telecommunication system of	Note cl 3. See also sub section (8).

		communications ….(c) the disclosure … of intercepted material or related communications data ….		the communications described in the warrant; … (d) the disclosure, in such manner as may be so described, of intercepted material obtained by any interception authorised or required by the warrant, and of related communications data.	
12(3)	Creates targeted examination warrants to access bulk intercept data	.. a warrant which authorizes the person.. to carry out the examination of intercepted material under a bulk interception warrant			This power is the consequence of clearly legislating bulk data powers. See mirror provisions in Part 6.
12(4)	Creates mutual assistance warrants		largely RIPA 5(1)(c)	the provision, in accordance with an international mutual assistance agreement, to the competent authorities of a country or territory outside the United Kingdom of any such assistance in connection with, or in the form of, an interception of communications as may be so described;	
12(8)	Allows for the extraction of communications data from what would otherwise be content		New definition – also see IPB subsections (6), (7) and (9)		It is questionable as to whether all forms of extraction would have been permitted under previous regime. Could involve detailed

					processing of content under CD powers.
13	Expands coverage of a single warrant from a single person or premises to multiple people, groups or premises. Also allows for training and testing		Broader than RIPA 8(1) Thematic warrants subject to criticism: ISC Report (paras 42 to 45), rec D; Anderson Rec 27. NB also provisions in CDB	Anderson Review suggested that specific interception warrants should be limited to a single person, premises or operation. In the case of an operation, each person or premises to which the warrant is to apply should be *individually specified* in a schedule to the warrant. ISC suggested that thematic warrants should be for a shorter timeframe than other targeted warrants, and should be used sparingly.	Allows for potentially lower levels of scrutiny of the individual placed under surveillance, if an entire group can be wrapped up together. How big can a 'group of persons who share a common purpose' be? Does this allow religious groups to be targeted? Note s. 23(4) for how this must be described in warrant. See *Szarbo and Vissy* v *Hungary* on importance of being able to identify subjects of surveillance (paras 66-67). What happens to data generated from testing and training, presumably performed on innocent individuals? No guidance on how individuals might be chosen. Consider impact of power of modification.

14	Requires the SoS to issue warrants personally on grounds specified in s. 14(3)	(a) in the interests of national security, (b) for the purpose of preventing or detecting serious crime, (c) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security (but see subsection (4)), or (d) for the purpose of giving effect to the provisions of an EU mutual assistance instrument….	redraft of RIPA 7 NB. amendments introduced by DRIPA	ISC recommended that Ministers should continue to be responsible, Rec. FF, GG. Anderson suggested that warrants should only be granted for the purposes of preventing or detecting serious crime (including giving effect to a MLAT) or in the interests of national security - Rec. 28 C	Tighter than original RIPA, as the economic well-being grounds are limited as per DRIPA. Use of intercept only for gathering evidence for legal proceedings is not allowed. The SoS has to consider for interception or mutual assistance warrants if the information could be obtained by other means. Cf *Zakharov* para 259; *Szarbo and Vissy* para 76. Note exception for urgent cases.
15	Lists those who can apply for warrants	(a) a person who is the head of an intelligence service; (b) the Director General of the National Crime Agency; (c) the Commissioner of Police of the metropolis; (d) the Chief Constable of the Police Service of Northern Ireland; (e) the Chief Constable of the Police Service of Scotland; (f) the Commissioners for Her Majesty's Revenue and Customs; (g) the Chief Defence	essentially as RIPA 6		

		Intelligence; (h) a person who is the competent authority of a country or territory outside the United Kingdom for the purposes of an EU mutual assistance instrument or an international mutual assistance agreement.			
16	Provides protection for parliamentarians		Replaces Wilson Doctrine. See Code of Practice on Interception Note IPT ruling in *Lucas* case	Note ISC Rec UU	Requires the PM's consultation for intercept of Parliamentarians. No requirement for PM's consent. Does not cover eg. London Mayor. Sensitive professions (e.g. doctors, journalists or lawyers) receive no special consideration as regards interception. Will the code cover this? It is not required by Schedule 6.
17	Allows Scottish Ministers to issue warrants		redraft of RIPA 7, with Scottish powers separated out		
18	Defines which applications are Scottish				

19	Requires warrants to be approved by judicial commissioners		All reviews made some comments on this. Anderson called for judicial authorisation. RUSI suggested judicial review.		Judges performing judicial review may be limited in what they can do. Under traditional judicial review, they are not asked to assess if they consider the application to be necessary and proportionate, merely that the decision that it was so was not unreasonable. However, the nature of judicial review enquiries has altered since HRA 1998, see *R (on the application of Lord Carlile of Berriew QC and others)* [2014] EWCA Civ 199. According to ECHR (e.g. *Zakharov*; *Szarbo and Vissy*) and Court of Justice jurisprudence, effective review is important.
19(2)	Establishes that the principles applied must be those of Judicial Review				See above

19(5)	Allows an appeal to the IPC if a judicial commissioner refuses approval				Even if a JC considers a decision unreasonable, this can be challenged
20	Allows urgent approval pre-judicial oversight		RIPA has urgency provisions: s 7(2).	Anderson suggested that provisions should be put in place for urgent cases, see Rec 31	Allows 5 days for the JC to make a decision; no requirement as to timing for the notification of the JC under subsection (2). Note *Szarbo and Vissy* paras 80-81. There should perhaps be particular monitoring of the frequency of urgent requests written into the legislation.
21	Deals with the consequences if a Judge refuses an urgent warrant	(2) The person to whom the warrant is addressed must, so far as is reasonably practicable, secure that anything in the process of being done under the warrant stops as soon as possible (3) the Judicial Commissioner who refused to approve the warrant may- (a) direct that any of the intercepted material or related communications data … is destroyed; (b) impose conditions as to the use or			Allows for, but does not require, deletion of data collected urgently and unreasonably. Allows an appeal to the IPC of that decision. No account taken of the target's views or interests, and no mechanism for redress.

		retention of any of that material or data.			
22	Allows senior officials to sign urgent warrants if SoS or Scottish Minister has expressly approved it		As RIPA 7(1)(b)		
23	Sets requirements for contents of warrants.		expanded version of RIPA 8		
24	Sets standard duration of warrants at 6 months, 5 days for urgent warrants	24(2) IPB	RIPA 9(6) sets these time limits for some warrants, and a shorter 3 month period for others	Note ISC Recommendation that thematic warrants should be for shorter period than other warrants	This is an extension of default time for warrants relating to crime or mutual assistance
25	Allows renewal of a warrant, with authorisation by a judicial commissioner if conditions justifying original issue of warrant remain.	s. 25(2)	Allowed for in RIPA 9		
26	Allows modification of warrants	..modifications that may be made under this section are- (a) adding or removing the name or description of a person organization or set of premises to which the warrant relates, (b) varying such name or description, and (c) adding, varying or removing any factor	RIPA 10	10 (2)If at any time the Secretary of State considers that any factor set out in a schedule to an interception warrant is no longer relevant for identifying communications which, in the case of that warrant, are likely to be or to include communications falling	Very broad power for change, especially in adding names or premises under (a). No requirement for judicial commissioner approval even to add multiple names. No express approval by the SoS is required, merely

		specified in the warrant in accordance with section 23(8)		within section 8(3)(a) or (b), it shall be his duty to modify the warrant by the deletion of that factor. (3) If at any time the Secretary of State considers that the material certified by a section 8(4) certificate includes any material the examination of which is no longer necessary as mentioned in any of paragraphs (a) to (c) of section 5(3), he shall modify the certificate so as to exclude that material from the certified material.	notification (see 5(c) and (11)). The requirements on the SoS to limit warrants in RIPA 10(2) and (3) are gone – note provisions on cancellation of the warrant as a whole in s. 27 IPB below.
27	Allows cancellation of warrants, and requires it on some occasions	(2) If any of the appropriate persons considers that- (a) a warrant issued under this Chapter is no longer necessary on any relevant grounds, or (b) that the conduct authorized by the warrant is no longer proportionate …, the person must cancel the warrant	RIPA 9(3)	The Secretary of State shall cancel an interception warrant if he is satisfied that the warrant is no longer necessary on grounds falling within section 5(3).	It seems that 27(2)(b) is new.
28	Allows officials to authorise and renew mutual assistance warrants for targets outside the UK				No reference to judicial oversight; decision may be delegated to senior official.

29-30	implementation and service of warrants		expanded versions of RIPA 11 (1-3)		Note extraterritoriality: s. 29(4), s. 30(2). Extraterritorial serving of interception warrants.
31	Requires operators to help with implementation	(3) Subsection (1) applies whether or not the relevant operator is in the United kingdom …	expanded version of RIPA 11(4) including the extraterritoriality provisions of DRIPA 4	Note comments in Anderson Report: operators are not happy with this (see 11.15-11.28)	Obligation to assist not limited to UK. Asserted under RIPA, expressly set out in s. 4 DRIPA.
31(4)	Specifies that operators do not have to do impractical things	The relevant operator is not required to take any steps which it is not reasonably practicable for the relevant operator to take	echoes RIPA 11(5)	A person who is under a duty by virtue of subsection (4) to take steps for giving effect to a warrant shall not be required to take any steps which it is not reasonably practicable for him to take.	Key issue when it comes to decryption requirements. What counts as 'reasonably practicable'?
31(5)	Provides some protection for overseas operators in case of conflict of law	(5) In determining … whether it is reasonably practicable for a relevant operator outside the United Kingdom to take any steps in a country or territory outside the United Kingdom for giving effect to a warrant, the matters to be taken into account include the following- (a) any requirements or restrictions under the law of that country	as per DRIPA 4(4)		Safeguard demanded by overseas operators and the subject of much detailed negotiation in DRIPA – issues about interpretation of this provision which accompanied the enactment of DRIPA remain.

		or territory that are relevant to the taking of those steps, and (b) the extent to which it is reasonably practicable to give effect to the warrant in a way that does not breach any of those requirements or restrictions			
31(8)	Allows for civil enforcement of warrants		RIPA 11(8), and specifying overseas as well, see s. 4(5) DRIPA.		
32-39	These next sections allow warrantless interception under various circumstances		see RIPA 3		
32(1)	Allows interception if sender and recipient have agreed		rephrase of RIPA 3(1)	(1) Conduct by any person consisting in the interception of a communication is authorised by this section if the communication is one which. . . is both— (a)a communication sent by a person who has consented to the interception; and (b) a communication the intended recipient of which has so consented.	
32(2)	Allows interception if one party has agreed, and surveillance		as in RIPA 3(2)	Conduct by any person consisting in the interception of	

	was authorised under Part 2 of RIPA			a communication is authorised by this section if— (a) the communication is one sent by, or intended for, a person who has consented to the interception; and (b) surveillance by means of that interception has been authorised under Part II.	
33	Allows interception for running postal or telecoms	(2) The purposes referred to in subsection (1) are- (a) purposes relating to the provision or operation of the service; 9b) purposes relating to the enforcement, in relation to the service, of any enactment relating to- (i) the use of postal or telecommunications services, or (ii) the content of communications transmitted by means of such services; (c) purposes relating to the provision of services or facilities aimed at preventing or restricting the viewing or publication or the content of communications transmitted by means of postal or telecommunications services.	As RIPA 3(3)	Conduct consisting in the interception of a communication is authorised by this section if— (a) it is conduct by or on behalf of a person who provides a postal service or a telecommunications service; and (b) it takes place for purposes connected with the provision or operation of that service or with the enforcement, in relation to that service, of any enactment relating to the use of postal services or telecommunications services.	Specifically allows interception to prevent particular material being transferred. This additional wording potentially prevents operators adopting an overly broad interpretation.

34	Allows businesses etc to monitor communications on their own equipment		Lawful Business Practice Regulations 2000		For example, to log outgoing emails.
35	Allows postal interception for enforcement of Postal Services Act and Terrorism Act, Schedule 7		Already allowed in that legislation.		
36	Allows OFCOM to intercept for maintaining wireless telegraphy		See Wireless Telegraphy Act 2006		
37	Allows interception in prisons to enforce prison rules		Note Code of Conduct		Are protections for legal communication etc. securely established in Prison Rules?
38	Allows interception in psychiatric hospitals				
39	Allows interception as requested by a foreign power	The Interception of a communication by a person in the course of its transmission … is authorized by this section if conditions A to D are met …(4) Condition C is that the interception is carried out in response to a request made in accordance with a relevant international agreement by the competent authorities of a country or territory outside the United Kingdom.	Power currently in s 94 telecoms Act 1984, though not aware this has ever been used for foreign requests.		Extremely broad power, with no supervision or signoff by ministers or judges. The explanatory notes suggest this would only cover individuals outside the UK. Condition C contains the overseas link, but it deals only with the originator of the request not the subject. Note Condition D requires

					further regulations to be made by SoS.
40	Aims to minimise the number of people accessing intercept material, and requires deletion when it is no longer needed		As RIPA s. 15	in relation to the intercepted material and any related communications data if each of the following— (a) the number of persons to whom any of the material or data is disclosed or otherwise made available, (b) the extent to which any of the material or data is disclosed or otherwise made available, (c) the extent to which any of the material or data is copied, and (d) the number of copies that are made, is limited to the minimum that is necessary for the authorised purposes. (3)… in relation to the intercepted material and any related communications data if each copy made of any of the material or data (if not destroyed earlier) is destroyed as soon as there are no longer any grounds for retaining it as necessary for any of the authorised purposes.	

41	Aims to replicate safeguards in 40 for data that goes overseas		RIPA 15	(6) Arrangements in relation to interception warrants which are made for the purposes of subsection (1)— (a) shall not be required to secure that the requirements of subsections (2) and (3) are satisfied in so far as they relate to any of the intercepted material … possession of which has been surrendered to any authorities of a country or territory outside the United Kingdom; but (b) shall be required to secure, in the case of every such warrant, that possession of the intercepted material .. is surrendered to authorities … only if the requirements of subsection (7) are satisfied. (7) The requirements of this subsection are satisfied .. if it appears to the Secretary of State— (a) that requirements corresponding to those of subsections (2) and (3) will apply, to such extent (if any) as	Stronger than the RIPA regime

				the Secretary of State thinks fit, … and (b) that restrictions are in force which would prevent, to such extent (if any) as the Secretary of State thinks fit, the doing of anything … which would result in such a disclosure as, could not be made in the United Kingdom.	
42	Bans reference or questioning of interception for legal proceedings or inquiries act		As RIPA s. 17		
Schedule 3	Ensures interception can be discussed in a range of legal setting, including at the IPT		As RIPA s. 18		Schedule 3 adds another exception.
43	Prevents unauthorised disclosures		As RIPA s.19		
43 (5)(g)	Allows SoS to direct operators to say how many warrants they have given effect to				Does not require such transparency direction
44	Creates offence of unauthorised disclosure		As RIPA s. 19		
45	Interpretations				

Part 3 Investigatory Powers Draft Bill - Review of drafting provenance – Investigatory Powers Research Group. This working document may be subject to change, following further assessment. For abbreviations and full source list go to bit.ly/ipbillsources. Comments/suggestions to: ipbillresearchgroup@gmail.com

IPB reference	Description of content	IPB extract	Source	Description in legislation / reviews	Issues/comments
46(1)(a) and 46(7)	Purposes for which obtaining communications data must be necessary before a warrant may be granted.	(1) ... if a designated senior officer of a relevant public authority considers - (a) that it is necessary to obtain communications data for a purpose falling within subsection (7)… [and] (c) that the conduct authorised by the authorisation is proportionate to what is sought to be achieved.' (7) '... if it is necessary and proportionate to obtain the data - (a) in the interests of national security; (b) for the purpose of preventing or detecting crime or of preventing disorder; (c) in the interests of the economic wellbeing of the UK so far as those interests are also relevant to the interest of national security; (d) in the interests of public safety; (e)	RIPA s 22(1) and (2) (with (3) and (5) in relation to proportionality) SI 2010/80 as amended. See Anderson review, Ch 15 para 52:'[t]he grounds on which communications data may be acquired should remain as set out in RIPA s22(2), subject to any limitation (relating, for example, to the need for crime to exceed a certain threshold of seriousness'; and para 55: '[a]n authorisation should be granted only if the DP is satisfied, having	Refers to a person designated for the purposes of this chapter not 'designated senior officer of a relevant public authority'. Refers to need to consider that obtaining data is 'necessary' but not 'proportionate': 'proportionate' is contained in s 22(5), which (in conjunction with s 22(3)) provides that a designated person cannot grant an authorisation unless he believes that obtaining the data by the conduct in question is 'proportionate to what is sought to be achieved'.	Does not contain (h)-(j). Communications data defined in cl 193 – see comments on that provision.

		for the purpose of protecting public health; (f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; (g) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; (h) to assist investigations into alleged miscarriages of justice; (i) where a person (P) has died or is unable to identify themselves because of a physical or mental condition, (i) to assist in identifying P or (ii) to obtain information about P's next of kin or other persons connected with P or about the reason for P's death or condition; (j) for the purpose of	taken the advice of the SPoC and considered all the matters specified in the application, that it is necessary and proportionate to do so'.		

		exercising functions relating to (i) the regulation of financial services and markets, or (ii) financial stability.'			
46(1)(b)	Limitation to specific investigation/operation or testing of systems/capabilities	Subsection (2) applies if a designated senior officer of a relevant public authority considers - ... (b) that it is necessary to obtain that data (i) for the purposes of a specific investigation or a specific operation, or (ii) for the purposes of testing, maintaining or developing equipment, systems or other capabilities relating to the availability or obtaining of communications data... NB. Sections 47(1)-(3) provide that a designated senior officer must not grant authorisation for the purposes of a specific investigation/operation if the officer is working on that investigation/operation unless 'exceptional	Potentially Anderson review at Ch 15 para 58	Recommends that designated persons 'should be required by statute to be independent from operations and investigations when granting authorisations related to those operations and investigations, and this requirement should be implemented in a manner consistent with the ECHR and EU law.'	Significance of introducing requirement regarding identification of a specific investigation or operation? Significance of expressly extending testing of systems/capabilities. How will subjects be chosen?

		circumstances' in subsection (3) apply.			
46(2)	Persons who may be authorised	The designated senior officer may authorise any officer of the authority…'	RIPA s 22(3)	Provides for the authorisation of 'persons holding offices, ranks or positions with the same relevant public authority as the designated person'	
46(2)	General nature of what may be authorised under an authorisation	The designated senior officer may authorise any officer of the authority to engage in any conduct which - (a) is for the purpose of obtaining the data from any person, and (b) relates to (i) a telecommunication system, or (ii) data derived from a telecommunication system.'	RIPA s 22(3) (with s 21(1) in relation to conduct)	Authorisation under s 22(3) relates to 'any conduct to which this Chapter applies' - this is set out in s 21(1), which states that the Chapter applies to 'any conduct in relation to a postal service or telecommunication system for obtaining communications data, other than conduct consisting in the interception of communications in the course of their transmission by means of such a service or system' (see below) and 'the disclosure to any person of communications data'	Is conduct which may be authorised any broader under the IPB, in light of both general wording and specific examples (see immediately below)? Note broadening through extension of definitions. Is 'data derived from a telecommunications system' in cl 46(2)(b)(ii) the same as 'communications data' in 46(1)(a) and 'data' in 46(1)(b) (bearing in mind definition of 'data' in cl 195)?
46(4)	Specific examples of what may be authorised	Authorised conduct may, in particular, consist of an authorised officer - (a) obtaining the	This seems to be a version of s. 22(3) and (4) of RIPA.		Does power to 'ask' for disclosure of data (as opposed to requiring via a notice) add

		communications data themselves from any person or telecommunication system; (b) asking any person whom the authorised officer believes is, or may be, in possession of the communications data to disclose it to a person identified by, or in accordance with, the authorisation; (c) asking any person whom the authorised officer believes is not in possession of the communications data but is capable of obtaining it to obtain it and disclose it to a person identified by, or in accordance with, the authorisation; or... [see immediately below in relation to notices] Note - s 46(6)(b) further provides that an authorisation may not authorise an authorised officer to ask/require the			anything new? What is the extent (if any) of the obligation to comply with a request, as opposed to a notice? Who may be 'asked'? The provision refers to 'person' (see general definitions), so the provision is not limited to service providers.

		disclosure of data to any person other than the authorised officer or an officer of the same relevant public authority.			
46(4)(d)	Specific examples of what may be authorised - Power to issue notices	Authorised conduct may, in particular, consist of an authorised officer - (d) requiring by notice a telecommunications operator (i) whom the authorised officer believes is, or may be, in possession of the communications data to disclose the data to a person identified by, or in accordance with, the authorisation, or (ii) whom the authorised officer believes is not in possession of the communications data but is capable of obtaining the data, to obtain it and disclose it to a person identified by, or in accordance with, the authorisation.' NB. See s 47(2) below in	RIPA s 22(4) See also Anderson review at Ch 15 para 53, recommending that '[t]he distinction between an authorisation and a notice (RIPA s22) is unnecessary and should be abandoned.'	Power to issue a notice arose where the <u>designated person</u> (rather than the authorised officer) believed that a telecommunications operator was or might be in possession of or capable of obtaining the communications data Notice could require the operator 'in any case, to disclose all of the data in his possession or subsequently obtained by him'	Significance of an officer authorised by the designated person, rather than the designated person him/herself, being able to issue a notice? Does this confer any more discretion on a 'lower level' decision-maker, or is the scope for discretion effectively removed by s 48(2) (below)? What is the significance of fact that it is no longer enough that the person with the power to issue a notice believe that the operator 'may be' capable of obtaining the data - must believe

		relation to matters to be included in any authorisation to issue a notice.			that they <u>are</u> so capable?
46(5)(a)	Authorisation may relate to data not in existence	An authorisation may relate to data whether or not in existence at the time of the authorisation'			Is this not covered by 'capable of obtaining'? Does this provision require providers to create the 'data' – and note provision refers to 'data' not 'communications data' (and note also 'data relating to the use of a telecommunications service' in cl. 46(5)(c)).
46(5)(b)	Authorisation may authorise conduct by persons other than authorised officers		Unknown/new		Consequences of broadening conduct authorised beyond conduct of the authorised officer?
46(6)	Limitation on persons to whom disclosure may be required	Provides that an authorisation may not authorise an authorised officer to ask/require the disclosure of data to any person other than the authorised officer or an officer of the same relevant public authority.	RIPA s 23(3)	Applies only to notices (as there is no express provision for requests pursuant to authorisations); provides that shall not require the disclosure of data to any person other than the person giving the notice or another specified person within the same relevant public authority	

46(6)(a)	Exclusion of interception from conduct authorised	An authorisation may not authorise any conduct consisting in the interception of communications in the course of their transmission by means of a telecommunication system'	RIPA s 21(1) Note also Anderson review at para 6.3ff in relation to the surprising breadth of what constitutes 'interception'	Excludes from definition of conduct to which the Chapter applies 'conduct consisting in the interception of communications in the course of their transmission by means of [a postal service or telecommunication system]'	
47(4)	Limitation on authorisations relating to 'internet communication records'	A designated senior officer of a relevant public authority which is not a local authority may not grant an authorisation for the purpose of obtaining data which is already held by a telecommunications operator and which is, or can only be obtained by processing, an internet connection record unless the purpose of obtaining the data is to identify - (a) which person or apparatus is using an internet service where (i) the service and time of use are already known, but (ii) the identity of the person or apparatus using the service is not known; (b) which internet	Unknown/new. NB. Query relevance of Anderson review Ch 15 para 15, which notes in relation to CDB the necessity 'to formulate an updated and coordinated position... on the operational case for adding web logs (or the equivalent for non-web based OTT applications) to the data categories currently specified in the Schedule to the Data Retention Regulations 2014 for the purposes of: (a) resolving shared IP	47(4)	Limitation on authorisations relating to 'internet communication records'. 'internet communication service' is not defined. Note definition of apparatus in cl. 195 and comments thereon. Is possession of 'material' in cl 47(4)(c) linked to digital material or does it include other materials?

		communications service is being used, and when and how it is being used, by a person or apparatus whose identity is already known, or (c) where or when a person or apparatus whose identity is already known is obtaining access to, or running, a computer file or computer program which wholly or mainly involves making available, or acquiring, material whose possession is a crime.' NB. Section 46(5) provides that a designated senior officer of a local authority may not grant authorisations of this kind at all. NB. Section 46(6) defines 'internet connection record'.	addresses or other identifiers (in particular, to identify the user of a website); (b) identifying when a person has communicated through a particular online service provider (so as to enable further enquiries to be pursued in relation to that provider); and/or (c) allowing websites visited by a person to be identified (to investigate possible criminal activity).'		
48(1)	Information authorisation must specify	An authorisation must specify - (a) the office, rank or position held by the designated senior officer granting it; (b) the matters falling within	RIPA s 23(1) and (2)	S 23(1) relates to authorisations and 23(2) to notices, which are dealt with together in the IPB because authorisation can be given <u>to issue</u> a notice	Requirements are substantively the same, with the following exceptions:- in relation to authorisations there is

		section 46(7) by reference to which it is granted [i.e. purposes]; (c) the conduct that is authorised; (d) the data or description of data to be obtained; and (e) the persons or descriptions of persons to whom the data is to be, or may be, disclosed or how to identify such persons.'			no requirement to specify the person(s) to whom the data is to be disclosed (this is accounted for by the fact that authorisations do not include a power to issue notices requiring disclosure); - in relation to notices there is an additional requirement to specify the manner in which any disclosure required by the notice is to be made.
48(2)	Additional requirements for authorisations authorising notices	An authorisation which authorises a person to impose requirements by notice on a telecommunications operator must specify - (a) the operator concerned, and (b) the nature of the requirements that are to be imposed, but need not specify the other contents of the notice.'	RIPA s 23(2)		
48(3)	Information notices must specify	The notice itself - (a) must specify (i) the office,	RIPA s 23(2)	Requires that the notice specify the communications data to be	Significance of the purpose of the notice

		rank or position held by the person giving it, (ii) the requirements that are being imposed, and (ii) the telecommunications operator on whom the requirements are being imposed…'		obtained/disclosed, the purpose by reference to which it was issued, and the manner in which any disclosure must be made Note that under IPB s 48(1) and (2) (see above) this information must (instead) be included in the authorisation authorising the issue of the notice	not being required to be included in the notice itself, meaning (presumably) the recipient may not know? This removes the possibility of a procedural check by the operator.
48(3)(b) and (4)	Writing requirements for authorisations and notices		RIPA s 23(1)(a) and (2)(a)	Terms substantively identical NB. See above re. exclusion of writing requirement in relation to authorisations/notices for which judicial approval is required; there appears to be no equivalent exclusion in the IPA	
49(1)	Duration of authorisations	(1) 'An authorisation ceases to have effect at the end of the period of one month beginning with the date on which it is granted.'	RIPA s 23(4)(a)	an authorisation or notice 'shall not authorise or require any data to be obtained after the end of the period of one month beginning with the date on which the authorisation is granted or the notice given'	Is effect of authorisation 'ceasing to have effect' precisely the same as its not being able to authorise the obtaining of any data?
49(2)-(3)	Renewal of authorisations	(2) 'An authorisation may be renewed at any time before the end of that period by the	RIPA s 23(5)-(7)	Terms substantively identical	

		grant of further authorisation.' (3) 'Subsection (1) has effect in relation to a renewed authorisation as if the period of one month mentioned in that subsection did not begin until the end of the period of one month applicable to the authorisation that is current at the time of the renewal.'			
49(4)-(6)	Duty to cancel authorisations	(4) 'A designated senior officer who has granted an authorisation must cancel it if the designated senior officer considers that the position is no longer as mentioned in section 46(1)(a), (b) and (c).' (5) The Secretary of State may by regulations provide for the person by whom any duty imposed by subsection (4) is to be performed in a case in which it would otherwise fall on a person who is no longer available to perform it.'	(compare) RIPA s 23(8)-(9)	Requirement relates only to notices rather than authorisations	Phrasing of requirement is different but effect appears to be the same, bar the absence in RIPA of the requirement re. specific investigation/ operation: authorisation must be cancelled where designated person satisfied that (a) 'it is no longer necessary on grounds falling within subsection (2) for the notice to be complied

		(6) 'Such regulations may, in particular, provide for the person on whom the duty is to fall to be a person appointed in accordance with the regulations.'			with', or (b) 'the conduct required by the notice is no longer proportionate to what is sought to be achieved'
49(7)	Effect on notice of authorisation expiring or being cancelled	A notice given in pursuance of an authorisation (and any requirement imposed by that notice) - (a) is not affected by the authorisation subsequently ceasing to have effect under subsection (1), but (b) is cancelled if the authorisation is cancelled under subsection (4).'	(compare) RIPA s 23(4)(a) and (b), RIPA s 23(5)-(7)	S 23(4): a notice 'shall not authorise or require any data to be obtained' after the end of a month, and 'shall not authorise or require any disclosure after the end of that period of any data not in the possession of, or obtained by, the postal or telecommunications operator at a time during that period' s 23(5)-(7) also provided for renewal of the notice itself	Do the two pieces of legislation operate in the same way? A notice under RIPA could not require disclosure past its period of validity (which does not appear to be the case under the IPB) but the notice itself could be renewed.
50(1)	Obligations of telecommunications operators to comply with notices	'It is the duty of a telecommunications operator on whom a requirement is imposed by a notice given in pursuance of an authorisation to comply with that requirement.'	RIPA s 22(6)	Terms substantively identical	
50(2)	Obligation of telecommunications operators to minimise data to be processed	'It is the duty of a telecommunications operator who is obtaining or disclosing communications data, in response to a request or	Potentially Anderson review at Ch 13 para 13.26(c)	[m]easures taken must be proportionate to the objective, meaning that the measure must be selected that least restricts human rights and	

		requirement for the data in pursuance of an authorisation, to obtain or disclose data in a way that minimises the amount of data that needs to be processed for the purpose concerned,'		that special care is taken to minimise the adverse impact of any measures on the rights of individuals, including in particular persons who are not suspected of any wrongdoing'	
50(3)	Limitation of duty to what is reasonably practicable	A person who is under a duty by virtue of subsection (1) or (2) is not required to do anything in pursuance of that duty that it is not reasonably practicable for that person to do.'	RIPA s 22(7)	Terms substantively identical	
50(4)	Enforcement of duty of telecommunications operators	The duty imposed by subsection (1) or (2) is enforceable by the Secretary of State by civil proceedings for an injunction, or for specific performance of a statutory duty…'	RIPA s 22(8)	Terms substantively identical	
51-53, 67	Filtering arrangements	[Too lengthy to reproduce]	Anderson review indicates at Ch 9 para 9.65ff that provision for a 'request filter' was made in the draft Communications Data Bill of 2012; see also Ch 14 para 14.25,		

			suggesting that the creation of a request filter was initially a proposal of the Joint Committee on the Draft Communications Data Bill in its report of December 2012		
54(1)-(5) (with Sch 4)	Identification of relevant public authorities and designated senior officers for the purposes of Art 46(3) and (8)	[Provisions bring Sch 4 into effect, which contains a table listing 'relevant public authorities' in column 1 and the minimum office/rank/position of the 'designated senior officer' for that authority in column 2]	RIPA s 25(1) and (2) (with 2010 Order) NB. See also Anderson review at Ch 15 paras 23 and 51	Some 'relevant public authorities' are listed in s 25(1) (police force, the National Crime Agency, HMRC, 'any of the intelligence services'); remainder, along with office/rank/position of 'designated person', are identified by Order Anderson review: 23: '[a]uthorisations for the acquisition of communications data otherwise than in bulk should be issued only on the authority of a DP authorised to do so by the authorising body.' 51: 'The issue of which (if any) categories of communications data should be unavailable	

				to certain public authorities should be reviewed, in the light of Recommendation 12 56: The RIPA Order 2010 (as it relates to designated persons) should be revised above and any revision of procedures for authorisation and review.'	
54(6)-(7) (with Sch 4)	Specific limitations on grants of authorisation by particular 'designated senior officers'	(6) 'A person who is a designated senior officer of a relevant public authority... may grant an authorisation... (a) only for obtaining communications data of the kind specified in the corresponding entry of column 3 of that table, and (b) only if section 46(1) is satisfied in relation to a purpose within one of the paragraphs of s 46(7) specified in the corresponding entry of column 4 of the table.' (7) 'Where there is more than one entry in relation to a relevant public authority in column 2 of the table, and a	RIPA Order 2010 para 5	Also restricts the purposes for which designated persons at particular public authorities may issue authorisations. Does <u>not</u> contain restriction regarding the type of communications data	More detailed comparison might reveal differences in the purposes for which authorisations can be granted by different public authorities.

		person is a designated senior officer of the authority by virtue of subsection (3) as it applies to more than one of those entries, subsection (6) applies in relation to each entry.' NB. ss 55-56 provides that the Secretary of State may by regulations modify s 54 or Sch 4.			
57(1)-(2), (4)-(5)	Designated senior officers of local public authorities	Makes specific provision for local public authorities as 'relevant public authorities' and identifies 'designated senior officers' as those holding the position of director, head of service or service manager (or a higher position). Subsection (5) provides for the Secretary of State to modify this position by regulation.	RIPA s 23A(6) (with RIPA Order 2010)	S 23A(6) defines a 'relevant person' as an individual holding an office/rank/position in a local authority; s 23A(5) requires that they be 'designated persons'; 2010 Order specifies Director, Head of Service, Service Manager or equivalent	
57(3)	Limitation on purposes for which designated senior officer at local public authority may grant authorisation	A designated senior officer of a local authority may grant an authorisation for obtaining communications data only if s 46(1)(a) is satisfied in relation	RIPA Order 2010 para 5 and table	Purpose for local authorities is also limited to (b) [i.e. for the purposes of detecting crime or preventing disorder]	Removal of limitation in previous regime means there has been an extension of data

		to a purpose within s 46(7)(b) [i.e. for the purposes of detecting crime or preventing disorder]			which local authorities can access.
58-59, 62-63	Additional provisions regarding powers of local authorities to grant authorisations	Local authorities to be party to a 'collaboration agreement' approved by the Secretary of State, as either a 'supplying authority' or a 'subscribing authority'. Authorisations may only be issued to officers of 'supplying authorities'.	See below re. police collaboration agreements under RIPA Note also Anderson Review at para 36	Anderson review recommends that 'procedures are streamlined, notably in relation to warrants and the authorisation of local authority requests for communications data'	The intended effect appears to be to encourage information-sharing between local authorities.
59	Need for judicial approval for local authority authorisations	An order of the 'relevant judicial authority' is required before an authorisation granted by the designated senior officer of a local authority takes effect (except in cases involving journalistic sources - see s 61). Subsection (3): the authority is not required to give notice of the application for an order to any person to whom the authorisation relates or to that person's legal representatives. Subsection (4) the relevant judicial authority may only	RIPA ss 23A, 23B NB. More detailed requirements are also provided in the Acquisition Code - relevant provisions are summarised in the Anderson review at p 112 NB. Contrast Anderson review at Ch 15 para 66, recommending that the requirement for judicial approval for	S 23A(1)-(5) RIPA provides that judicial authorisation is required wherever a 'relevant person', defined as an official at a local authority, has granted or renewed an authorisation or given or renewed a notice. Approval is only to be given on essentially the same basis as under the IPB, though wording of (b) is that 'at the time... there remain reasonable grounds for believing that the requirements of section 22(1) and (5) are satisfied in relation to the authorisation'.	

		approve the authorisation if it considers that '(a) at the time of the grant, there were reasonable grounds for considering that the requirements of this Part were satisfied in relation to the authorisation, and (b) at the time when the relevant judicial authority is considering the matter, there are reasonable grounds for considering that the requirements of this Part would be satisfied if an equivalent new authorisation were granted at that time.' Subsection (7) provides that in England and Wales the 'relevant judicial authority' means a justice of the peace.	local authority requests should be abandoned and instead '[a]pprovals should be granted, after consultation with NAFN, by a DP of appropriate seniority within the requesting public authority.'	In addition, the relevant judicial authority must be satisfied that the 'relevant conditions' are satisfied in relation to the authorisation; these are (i) that the individual was a designated person, (ii) that the grant/giving/renewal was not in breach of any restrictions imposed by the Secretary of State under s 25(3), and that (iii) any other conditions provided for by an order of the Secretary of State were satisfied. These conditions may well be covered by the use in the IPB of the broad phrase 'the requirements of this Part'. The relevant judicial authority is also a justice of the peace in England and Wales. As under the IPB, notice to the person to whom the authorisation relates/their representatives is not required. NB. The requirement that the authorisation be in	

				writing/leave a record does not apply in respect of an authorisation or notice requiring judicial approval	
60	Requirement to consult a 'single point of contact'	(1) 'Before granting an authorisation, the designated senior officer must consult a person who is acting as a single point of contact.' (2) 'But, if the designated senior officer considers that there are exceptional circumstances which mean that subsection (1) should not apply in a particular case, that subsection does not apply in that case.' (3) 'Examples of exceptional circumstances include - (a) an imminent threat to life or another emergency, or (b) the interests of national security.' .... (5)-(7) [Contain examples of what single point of contact may advise on.]	Acquisition Code (see Anderson review at Ch 6 para 6.65ff) Anderson review at Ch 15 para 61 ff also recommends use of single points of contact	Anderson report recommends that no authorisation should be granted without the prior opinion of a single point of contact (SPoC), whose functions should be set out in statute along the lines set down in the Acquisition Code. Anderson recommends that SPoC need not be located within the requesting authority.	
61	Requirement for judicial authorisation to identify/confirm journalistic sources	[Too lengthy to reproduce]	(compare) Anderson review at Ch 15 paras 67-69	Recommends (1) special consideration is given to the possible consequences for the exercise of rights and	There are concerns about the scope of this provision. It relates to communications data,

			NB. Draft Interception Code - see Anderson review at Ch 6 para 6.79 NB. The Anderson review at Ch 6 para 6.80 suggests that the Acquisition Code provided that it may be possible to 'infer an issue of sensitivity from the fact that someone has regular contact with, for example, a lawyer or journalist' and that in such circumstances 'special consideration' should be given to necessity and proportionality. Anderson also notes that 'in cases where an application is made for communications data in order to identify a journalist's source, judicial authorisation must be obtained via	freedoms, (2) appropriate arrangements are in place for the use of the data, and (3) the application is flagged for the attention of ISIC inspectors. If data is sought for the purpose of determining confidential matters, e.g. the identity of a source, the designated person 'should be obliged either to refuse the request or to refer the matter to ISIC for a Judicial Commissioner to decide whether to authorise the request.' Note PACE and Acquisitions Code.	not interception or mass surveillance. It does not apply to security services. See also *Telegraaf Media Nederland Landelijke Media BV* v. *NL* (39315/06) (ECHR). There are no equivalent protections specified in the draft bill for other sensitive profession, although Schedule 6 provides for a Code of Conduct in relation to this part. At para (4) it requires the code to include '(a) provision designed to protect the public interest in the confidentiality of sources of journalistic information, and (b) provision about particular considerations applicable to any data which relates to a member of a

			the procedures in PACE'. NB. See also Anderson review at Ch 12 para 12.61ff for concerns raised in submissions relating to journalistic material		profession which routinely holds legally privileged information or relevant confidential information'.
64	Police collaboration agreements	(1) [Section applies if chief officer of a police force in England and Wales has entered into a 'police collaboration agreement' (defined as an agreement under s 22A of the Police Act 1996) pursuant to which (i) a designated senior officer of force 1 is permitted to grant authorisations to officers of a collaborating force, (ii) officers of force 1 may be granted authorisations by a designated senior officer of a collaborating force, or (iii) officers of force 1 act as single points of contact for officers of a collaborating force.] (2) [Persons by/to whom	RIPA s 22(3A)-(3I), 23(3A)-(3C)	Reference is to s 23(1) of the Police Act 1996 rather than s 22A Covers options (i) and (ii) only (as there are no provisions for single points of contact in RIPA)	

		authorisations may be granted are additional to those by/to whom authorisations could otherwise be granted under Part 3.]			
65(1)	Lawfulness of conduct authorised by Part 3	Conduct is lawful for all purposes if - (a) it is conduct in which any person is authorised to engage by an authorisation or required to undertake by virtue of a notice given in pursuance of an authorisation, and (b) the conduct is in accordance with, or in pursuance of, the authorisation or the notice.'	RIPA s 21(2)	Terms substantively identical	
65(2)	Civil liability in respect of conduct authorised by Part 3	A person (whether or not the person authorised or required) is not to be subject to any civil liability in respect of conduct that - (a) is incidental to or is reasonably undertaken in connection with conduct that is lawful by virtue of subsection (1), and (b) is not itself conduct for which an authorisation or	RIPA s 21(3)	Does not contain phrase 'whether or not the person authorised or required' Does not contain phrase 'or is reasonably undertaken in connection with'	Scope of civil immunity has clearly been expanded both in terms of subjects and in terms of conduct. Would this protect operators from their duty at s. 50(2) IPB?

		warrant (i) is capable of being granted under any of the enactments mentioned in subsection (3), and (ii) might reasonably have been expected to have been sought in the case in question.'			
66	Offence of making 'unauthorised disclosure'	(1) 'It is an offence for a telecommunications operator, or any person employed for the purposes of the business of a telecommunications operator, to disclose, without reasonable excuse, to any person the existence of - (a) any requirement imposed on the operator by virtue of this Part to disclose communications data relating to that person, or (b) any request made in pursuance of an authorisation for the operator to disclose such data.'	(compare) RIPA s 19, which contains an offence consisting of unauthorised disclosure of the existence and contents of warrants for interception		Significance of extending criminal liability for disclosure in relation to notices?
69	Extraterritorial application of Part 3	(1) 'An authorisation may relate to conduct outside the UK and persons outside the UK'	RIPA ss. 22(5A) and (5B) Anderson review at Ch 15 para 25	Terms substantively identical to subsections (1)-(4) <u>No</u> equivalent of subsections (4) or (5)	Significance of addition of subsections (4) or (5)? (4) is a conflict of laws protection, which has been lobbied for

		(2) 'A notice given in pursuance of an authorisation may relate to conduct outside the UK and persons outside the UK' (3) [Provides for means of delivering notices] (4) 'In determining for the purposes of subsection (3) of s 50 whether it is reasonably practicable for a telecommunications operator outside the UK to take any steps in a country or territory outside the UK for the purpose of complying with a duty imposed by virtue of subsection (1) or (2) of that section, the matters to be taken into account include the following - (a) any requirements or restrictions under the law of that country or territory that are relevant to the taking of those steps, and (b) the extent to which it is reasonably practicable to	Note also Anderson review at Introduction para 1.4(b), identifying one of the reasons for the passage of DRIPA as being 'the need to put beyond doubt the extraterritorial effect of warrants, authorisations and requirements relating to interception and communications data, so that they could for example be served on overseas service providers'.	Anderson review recommends that 'extraterritorial application should continue to be asserted in relation to warrants and authorisations (DRIPA 2014 s4), and consideration should be given to extraterritorial enforcement in appropriate cases' NB. S 22(6), relating to the obligations arising from the issuing of a notice, specifically provides that it is the duty of a telecommunications operator 'whether or not the operator is in the UK' to comply with the requirements of the notice - the same effect appears to be achieved, implicitly if not expressly, by IPB s 50 (see above)	by industry. For (5) need to cross-refer to 193(10), which provides a territorial basis for inclusion, so it implies that requests for communications data can be made even where the operator has no territorial link, which seems significant.

		comply with the duty in a way that does not breach any of those requirements or restrictions.' (5) 'Nothing in the definition of 'telecommunications operator' limits the type of communications data in relation to which an authorisation, or a request or requirement of a kind which gives rise to a duty under section 50(1) or (2), may apply.'			

Part 4 Investigatory Powers Draft Bill - Review of drafting provenance – Investigatory Powers Research Group. This working document may be subject to change, following further assessment. For abbreviations and full source list go to bit.ly/ipbillsources. Comments/suggestions to: ipbillresearchgroup@gmail.com.

IPB reference	Description of content	IPB extract	Source	Description in legislation/reviews	Issues/comments
71	Powers to require retention of certain data (General) - identifies what retention notices may require and to whom they may apply, as well as their duration.	S.71(1) The Secretary of State may by notice (a "retention notice") require a telecommunications operator to retain relevant communications data if the Secretary of State considers that the requirement is necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (j) of section 46(7) (purposes for which communications data may be obtained). (3) A retention notice must not require any data to be retained for	See Regulation of Investigatory Powers Act 2000, s.23 See Data Retention and Investigatory Powers Act 2014, s.1	IP Bill Explanatory Notes: S.71(3) "This clause provides a power to require communications service providers to retain communications data … for which it can be acquired for a maximum period of 12 months". S.71 (9) "Such communications data would include phone numbers, email addresses and source IP addresses." S.71 (9)(f) "Provides for the retention of internet connection records. ... They could be used, for example, to demonstrate a certain device had accessed an online communications service but they would not be able to be used to identify what the	The maximum retention period of 12 months replicates the scope established under section 1(5) of the DRIPA 2014 (and the recommendation of the Advocate General's Opinion in the CJEU judgment of *Digital Rights Ireland*). Note reference from the Court of Appeal in *SoS* v *Davis & Ors* with regard to s. 1 DRIPA. 'telecommunications operator' is defined in cl. 193(10) and 'communications data' is defined at cl 193(5). Note expanded definitions. A retention notice may require (cl 71(2)(b)) the retention of 'all data' – presumably 'communications' data' and not 'data' as defined in cl. 195. Cl. 71(9) seems broader than previously. While the

		more than 12 months ..... S.71(9) In this Part "relevant communications data" means communications data which may be used to identify, or assist in identifying, any of the following— (a) the sender or recipient of a communication (whether or not a person), (b) the time or duration of a communication, (c) the type, method or pattern, or fact, of communication, (d) the telecommunication system (or any part of it) from, to or through which, or by means of which, a communication is or may be transmitted,		individual did on that service. … Clause 193 provides that in the particular context of web browsing anything beyond data which identifies the telecommunication service (e.g. bbc.co.uk) is content." Note earlier provisions in CPB	Explanatory memorandum refers to internet connection records the phrasing in cl 71(9)(f) is not limited to ICRs. Note definition of 'identifier': limited to cl 71(9).

		(e) the location of any such system, or (f) the internet protocol address, or other identifier, of any apparatus to which a communication is transmitted for the purpose of obtaining access to, or running, a computer file or computer program. In this subsection "identifier" means an identifier used to facilitate the transmission of a communication.			
72	Matters to be taken into account before giving retention notices (Safeguards)	S.72(1) Before giving a retention notice, the Secretary of State must, among other matters, take into account— (a) the likely benefits of the notice, (b) the likely number of users (if known) of	New (IP Bill) - S.72(1) However, s.72(2) of the IP Bill draws from s.2(2) of the Communications Data Bill 2012		See also similar provisions in Part 6.

		any telecommunications service to which the notice relates, (c) the technical feasibility of complying with the notice, (d) the likely cost of complying with the notice, and (e) any other effect of the notice on the telecommunications operator (or description of operators) to whom it relates. S.72(2) Before giving such a notice, the Secretary of State must take reasonable steps to consult any operator to whom it relates.			
73	Review by the Secretary of State (Safeguards)	S.73(1) A telecommunications operator to whom a retention notice is given may, within such	See Communications Data Bill 2012, s.7	IP Bill Explanatory Notes: "This clause permits the recipient of a notice to refer the notice back to the	This provision is significant for explicitly providing the private sector with a means to challenge the necessity and/or proportionality of a

		period or circumstances as may be provided for by regulations made by the Secretary of State, refer the notice back to the Secretary of State. (see Bill for full text)		Secretary of State where the recipient of the notice considers an obligation unreasonable. Subsection (1) states that the provider will have the opportunity to refer a notice either within a specified time period or specified circumstances which will be set out in the regulations. Subsection (4) states that the person is not required to comply with the specific obligations under referral until the notice has been reviewed by the Secretary of State. The actions that the Secretary of State must take in reviewing the notice and the role of the Technical Advisory Board and the Investigatory Powers Commissioner are outlined at subsections (5-8). Subsection (9) requires the Commissioner and the Technical Advisory Board to	notice made by the Secretary of State. It could further enhance the oversight of the IP Bill (and its effectiveness) if such objections (and the subsequent responses, esp. that of the Technical Advisory Board and IPC) are recorded and made publicly available in the Annual Reports of the Investigatory Powers Commissioner.

				consult the operator and report their conclusions to the operator and Secretary of State. After consideration of the conclusions of the Commissioner and Board, the Secretary of State may decide to confirm the effect of the notice, vary the notice or withdraw it. Subsection (12) imposes an obligation on the Secretary of State to keep a notice under review, regardless of whether or not it has been referred."	
74	Data integrity and security (Safeguards)	S.74(1) A telecommunications operator who retains relevant communications data by virtue of this Part must— (a) secure that the data is of the same integrity, and subject to at least the same security and protection, as the data	See Communications Data Bill 2012, s.3 See Data Retention and Investigatory Powers Act 2014, s.1(4)(d)	IP Bill Explanatory Notes: "This clause requires data retained by virtue of this legislation must be kept securely and, once the retention period expires, deleted in a way that ensures access is impossible."	The ECJ in *Digital Rights* implies that the security standard is higher than for other data, e.g. para. 66. s. 74(2) seems too unspecific in terms of the circumstances in which retained data should be deleted (looking at paras 255, 282 & 302 of the recent ECtHR judgment in *Zakharov* in particular).

		on any system from which it is derived, (b) secure, by appropriate technical and organisational measures, that the data can be accessed only by specially authorised personnel, and (c) protect, by appropriate technical and organisational measures, the data against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful retention, processing, access or disclosure. S.74(2) A telecommunications operator who retains relevant communications data by virtue of this Part must destroy the data			

		if the retention of the data ceases to be authorised by virtue of this Part and is not otherwise authorised by law. S.74(3) The requirement in subsection (2) to destroy the data is a requirement to delete the data in such a way as to make access to the data impossible. S.74(5) The deletion of the data may take place at such monthly or shorter intervals as appear to the operator to be practicable.			
75	Disclosure of retained data (Safeguards)	A telecommunications operator must put in place adequate security systems (including technical and organisational			

		measures) governing access to relevant communications data retained by virtue of this Part in order to protect against any unlawful disclosure.			
76	Variation or revocation of notices	S.76(1) The Secretary of State may vary a retention notice. S.76(4) A retention notice may not be varied so as to require the retention of additional relevant communications data unless the Secretary of State considers that the requirement is necessary and proportionate for one or more of the purposes falling within paragraphs (a) to (j) of section 46(7) (purposes for which communications data may be obtained).	See Data Retention and Investigatory Powers Act 2014, s.1(4)(b)	IP Bill Explanatory Notes: "Subsections (1)-(8) provide for the Secretary of State to vary a notice. Where a notice is varied the same considerations will apply as in the giving of a notice. Subsections (9)-(12) provide for the revocation of data retention notices in full or in part."	S.76(12) prevents an operator challenging a retention notice purely on the basis of a prior revocation. This policy allows for considerable divergence in the treatment of operators and may hinder the development of best practice, but may also allow for less onerous requirements to be placed on operators of a smaller scale (e.g. SMEs) More detail to be provided in IP Bill's Codes of Practice. See schedule 6. There is no specific paragraph dealing with the code under part 4.

		S.76(9) The Secretary of State may revoke (whether wholly or in part) a retention notice. S.76(12) The fact that a retention notice has been revoked in relation to a particular description of communications data and a particular operator (or description of operators) does not prevent the giving of another retention notice in relation to the same description of data and the same operator (or description of operators).			
77	Enforcement of notices and certain other requirements and restrictions	S.77(1) It is the duty of a telecommunications operator on whom a requirement or	See Regulation of Investigatory Powers Act 2000, s.22 See Communications	IP Bill Explanatory Notes: "This clause provides a power to the Secretary of State to enforce compliance of notices	

		restriction is imposed by— (a) a retention notice, or (b) section 74 or 75, 40 to comply with the requirement or restriction. S.77(2) A telecommunications operator, ..., must not disclose the existence and contents of a retention notice to any other person. S.77(3) The duty under subsection (1) or (2) is enforceable by civil proceedings	Data Bill 2012, s.8 See Data Retention and Investigatory Powers Act 2014, s.1(4)	and other matters by civil proceedings."	
78	Application of Part 4 to postal operators and postal services - so that references to telecommunications operators, services etc are to be understood as postal operators, services etc		See Communications Data Bill 2012, s.25	IP Bill Explanatory Notes "This clause specifies that the provisions of this Part also apply to postal services."	
79	Extra-territorial application of Part 4	S.79(1) A retention notice,..., may relate to conduct outside the United Kingdom and	See Regulation of Investigatory Powers Act 2000, ss.11 and 12, (as amended by	IP Bill Explanatory Notes "This provides that communications service	This is an important limitation on the extra-territorial impact of Part 4, going beyond the

		persons outside the United Kingdom. S.79(2) Section 77(1) has effect, in relation to a requirement or restriction imposed by virtue of a retention notice or by section 74 or 75 and which relates to conduct or persons outside the United Kingdom, as a duty to have regard to the requirement or restriction (rather than comply with it).	Data Retention and Investigatory Powers Act 2014, s.4)	providers based outside the United Kingdom, but providing services to customers based within the United Kingdom, can retain relevant communications data related to such customers. The communications service provider based outside the United Kingdom has a duty to give regard to the requirement but they cannot be compelled to comply with it."	conflict of laws provisions in other parts.
80	Part 4: interpretation	S.80(1) In this Part—"notice" means notice in writing, "relevant communications data" has the meaning given by section 71(9), "retention notice" has the meaning given by section 71(1). S.80(2) See also—section 193	New (IP Bill)	IP Bill Explanatory Notes "This clause provides for interpretation of this Part, including references for relevant definitions."	

		(telecommunications definitions), section 194 (postal definitions), section 195 (general definitions).			

Part 5 Investigatory Powers Draft Bill - Review of drafting provenance – Investigatory Powers Research Group. This working document may be subject to change, following further assessment. For abbreviations and full source list go to bit.ly/ipbillsources. Comments/suggestions to: ipbillresearchgroup@gmail.com.

IPB reference	Description of content	IPB extract	Source	Description in legislation / reviews	Issues/comments
81(1)	Establishes two types of warrant		see below	ISC Report Rec CC	
81(2), (3), (4), (5)	Creates targeted equipment interference warrants		government claims ISA sec 5; Equipment Interference (EI) Code of Practice sec 4	New in legislation	ISA Sec. 5 is a broad power for property interference that does not clearly include equipment interference; the sections also provide significantly more detail on the subject matter of the warrant than the Code of Practice does. ISA 1994 also only applies to GCHQ.
81(6), (7), (8)	A targeted EI warrant may not authorise interception				Note however that sub section (4) permits 'monitoring observing or listening to a person's communications or other activities'. Potentially this is a wider intrusion than intercepting telecommunications.
81(9)	Creates targeted examination warrants		New		No parallel previously existed for ISA sec. 7 ((7) only relates to outside UK). See comments by ISC report about means of choosing what to examine and Rec J.
81(10)	EI warrants can be combined with certain other warrants, such as interception warrants		EI Code sec 4.5 explicitly provides for the combination of EI warrants with directed or		

			intrusive surveillance warrants under RIPA		
82	Defines "equipment data"		New		
83	Subject matter of warrants		ISA sec 5 (but see comment)	See ISC Rec D	This is much broader than the language of ISA sec. 5, and has been explicitly designed to cover all "thematic" EI warrants that do not specify the person or equipment to be targeted
84	Power to issue warrants to intelligence services		similar to EI Code sec 4		See differences with EI Code, especially the addition of Judicial Commissioners
84(4), (5)	Grounds on which warrant is declared "necessary"		ISA sec 5; EI Code sec 2		Economic well-being is circumscribed in the IPB.
84(6)	Must consider if what is sought to be achieved by warrant could reasonably be achieved by other means		EI Code secs 2.7, 4.7		Should this be strengthened as a power of last resort?
85	Additional protections for members of Parliament		replaces Wilson doctrine		What about journalists and other sensitive professions. Will this be dealt with by Code? Schedule 6 requires the position of these groups to be taken into account only in respect of communications data. A code may nonetheless deal with this issue.
86	Power to issue warrants to intelligence services, Scottish Ministers				ISA sec 5 puts power in Secretary of State, does not specify Scotland
87	Power to issue warrants to the Chief of Defence Intelligence				ISA does not mention the Chief of Defence Intelligence
88	Decision to issue warrant to be taken personally by Minister		EI Code sec 4	See also ISC Rec FF	EI Code allows for delegation in urgent situations

89	Power to issue warrants to law enforcement officers		Government claims the Police Act 1997		The Police Act is also broad, much like ISA sec 5
90	Approval of warrants by Judicial Commissioners		Suggested by Anderson. Partially supported by RUSI.		Judicial review standard does not allow for a full, substantive authorisation process
91	Approval of warrants in urgent cases		EI Code sec 4		EI Code has an urgent approval process, but since Judicial Commissioners were not contemplated, it differ significantly from the current bill
92	Warrants ceasing to have effect under section 91				Only must cease EI as soon as possible, "so far as reasonably practicable"; destruction of material previously obtained under the warrant is not automatic. Consider *Zakharov* on the destruction of material generally.
93	Requirements that must be met by warrants		EI Code sec 4		Because of the expanded subject matter of the warrants this section differs from the EI Code. It seems more detailed than other sections on the requirements to be met by warrants under other parts of the bill
94	Duration of warrants		EI Code sec 4		
95	Renewal of warrants		EI Code sec 4		More detail in Bill than in EI Code
96, 97	Modification of warrants				Not mentioned in EI Code
98	Cancellation of warrants		EI Code sec 4		
99	Implementation of warrants				Not in EI Code
100	Service of warrants				Not in EI Code

101	Duty on telecommunications providers to assist with implementation	The relevant operator is not required to take any steps which it is not reasonably practicable for the relevant operator to take			Not in EI Code; this power is troubling in that it could further undermine security by, for instance, allowing a requirement that a telecom operator send out a false security update to facilitate the EI. Note this only applies to a public telecommunications operator, or 'a person … who has control of the whole or any part of a public telecommunications system located wholly or partly in or controlled from, the United Kingdom' (sub section (5)(b)).
102	Offence of making unauthorised disclosure				Not in EI Code, also sec 6 limits disclosure. Makes it very difficult to understand and vet the hacking techniques being used.
103	Safeguards for material obtained		EI Code sec 6		There are some differences between the EI Code and the Bill
104	Restriction on issues of EI warrants to certain law enforcement officers				See above, police power to conduct EI only recently avowed; need to compare with reach of Police Act 1997
105	Definitions	"'communication' includes (a) anything comprising speech, music, sounds, visual images or data of any description, and (b) signals			This is the same as the definition in cl 193, which is there expressed to be in relation to a telecommunications operator. Note the possibility for 'things' to communicate. Note definition of 'apparatus' in cl 195; the position of software is not clear.

		serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus"			'Equipment' is defined very broadly as it includes devices producing emissions of any sort and any device capable of being connected thereto.

Part 6 Chapter 1 Investigatory Powers Draft Bill - Review of drafting provenance – Investigatory Powers Research Group. This working document may be subject to change, following further assessment. For abbreviations and full source list go to bit.ly/ipbillsources. Comments/suggestions to: ipbillresearchgroup@gmail.com.

IPB reference	Description of content	IPB extract	Source	Description in legislation / reviews	Issues/comments
107			RIPA S.6		Restricted to national security or serious crime/ economic well-being of UK combined with national security. Application by head of an intelligence service only (NARROWER)
106(2), 107(1)(a)	overseas-related communications	106(3) Communications sent by or received by individuals who are outside the British Islands	s. 20 RIPA	20 RIPA "external communication" means a communication sent or received outside the British Islands; Anderson 5.35 to 5.36, 5.38, 6.42 to 6.59, 5.90, 7.30, 8.63, 10.22, 11.36, 12.25, 12.29, 12.38, 14.40, 14.76, 14.77, Recommendation 44	REPLACEMENT. External/internal communications distinction replaced; but does it solve the problems? Does it fully implement Anderson Recommendation 44? Does it exclude device-initiated communications?
111, 119	Operational purposes	111(3) Bulk interception warrant must specify the operational purposes for which any intercepted material or related	RIPA	RIPA: RIPA S8(4) certificate replaced by 'specified operational purposes' stated in	REPLACEMENT (application to related communications data is NEW)

		communications data obtained under the warrant may be selected for examination. 111 (4) it is not sufficient simply to use the descriptions contained in 107(1)(b) or (2), but 'the purposes may still be general purposes'. Examination must be for the specified operational purposes 119(1) and (2)		warrant; applies to related communications data as well as intercepted material. Certificate (but only applicable to intercepted material, not related communication data.); Anderson ES 14(b) 14.75, Recommendations 43, 45 ISC recommended publication of certificate (Recommendation N)	
106(2)(b), 106(4)(b) and 107(1)(a)(ii)	related communications data	*Description (106)* Purpose: 'any one or more of': (2)(b) obtaining of related communications data from overseas-related communications Warrant authorises: 'any one or more of': (4)(b)obtaining of related communications data from communications described in the warrant	RIPA 5(6)(b)	RIPA 'conduct for obtaining related communications data' ['and'] "related communications data", in relation to a communication intercepted in the course of its transmission … means	Currently RIPA enables bulk interception of related communications data only collaterally to bulk interception of content. IPB empowers a 'related communications data only' warrant. (NEW)

		Power to issue (107) SoS considers purpose is 'one or more of': (1)(a)(ii) obtaining of related communications data from overseas-related communications. "(6) In this Chapter "related communications data", in relation to a communication transmitted by means of a telecommunication system, means data falling within subsection (7) or (8)." Related communications data can apparently be sourced from elsewhere than the bulk interception (contrast 106(6) with 12(6)(b); and see EN 271 and 272.) Cf 195(1) "Data" includes any information which is not data.		so much of any communications data … as- (a) is obtained by, or in connection with, the interception; and (b) relates to the communication or to the sender or recipient, or intended recipient, of the communication;"; Anderson 10.40(a) to (c), 14.46, 14.73, 20(b), Recommendation 42.	But nothing in IPB to say default in preference to a full content warrant? Could be used to obtain related communications data without an interception?
106(6) and (7)	Scope of 'related communications data'	"related communications data", in relation to a communication transmitted by means of a telecommunication system,			NEW

		means data falling within subsection (7) or (8). 106(7)(b): … data as … enables or facilitates the functioning of any telecommunication system or any telecommunications service provided by means of a telecommunication system			
106(8) and (9)	content definition	106(8) and (9): content that if it were logically separated from the remainder of the content of the communication "would not reveal anything of what might reasonably be expected to be the meaning of the communication, … and would be … (a) Data which may be used to identify, or assist in identifying, any person, apparatus, telecommunication system or telecommunications service, and (b) data which describes an event or the location of any person, event or thing"		Anderson 7.24, 10.28, 10.40, Annex 2, Annex 7 (7) ISC 80, 142-143, Recommendation AAA.	Includes some kinds of data extracted from intercepted content. Once extracted does that data cease to be 'content' and thus is not 'intercepted material'? (See below concerning restrictions on examination of intercepted material) Cf NEW 193(6) Definition of "Content": … elements … which reveal anything of what might reasonably be expected to be the meaning of the communication…"
	Examples	EN 275: examples of non-communications data that would fall within the extended meaning of 'related communications data':			.

		"(a) The version of the app sending the message; (b) Data relating to any files attached to a message such as the date and time it was created and the author; (c) Any location information related to the communication, for example the location required to enable an application; (d) Any email addresses contained within a communication.			
106(5)(a)(ii)	Authorises collateral interception of non-overseas-related communications (similar to RIPA).	Authorises any conduct which it is necessary to undertake in order to do what is expressly authorised or required by the warrant including "the interception of communications not described in the warrant"	RIPA 5(6)(a)	5(6)(a) "all such conduct (including the interception of communications not identified by the warrant) as it is necessary to undertake in order to do what is expressly authorised or required by the warrant"; Ditto. ISC para 112(v) states that if the agencies realise that what they are examining is a	Overseas-related and collaterally intercepted domestic communications form a common pool of intercepted material. Similarly to RIPA, no requirement to attempt to separate or discard domestic communication. Collateral interception of related communications data discussed in *Liberty v GCHQ* IPT judgment [66], [106] to [114], [138] to [139].

				domestic communication they must cease examining it and apply for a targeted RIPA interception warrant; and that the 16(3) modification is not available. While this would accord with the overall purpose of S.8(4) warrants nowhere is this explicitly stated in RIPA.	
106(2)(b) and 106(5)(a)(ii)	Authorises necessary collateral interception of related communications data, similar to RIPA.	106(2)(a) "Obtaining of related communications data from [overseas-related] communications; 106(5)(a)(ii): "conduct for obtaining related communications data from … [non-overseas-related communications intercepted under 106(5)(a) (i)]"		RIPA 5(6)(b) "conduct for obtaining related communications data"	Selection criteria (below) apply only to 'intercepted material' (119(1)(c)). Potential for creating profiles of internet users generally, including UK users? (but NB *Liberty and Others v GCHQ* IPT judgment at [139] and IOCCO 2014 Annual Report at 6.63 to 6.65).
119(1)(c),(3)(a)and(4)	Selection criteria for examination of intercepted material:	121(1) 'intercepted material' includes only content.	RIPA S16(2)		Restrictions on examination of content broadly equivalent to RIPA (subject to possible effect of

	referable to an individual known to be in BI at that time; and purpose of using criteria is to identify the content of communications sent by, or intended for, that individual.	NEW 193(6) definition of 'content';			new definitions of content and related communications data).
119(3)(b) to (d)	Exceptions to selection restrictions	Addressee of warrant considers that selection restrictions would not be breached by selection for examination (119(3)(b))	RIPA	"believes, on reasonable grounds, that the circumstances are such that the material would" fall outside the selection restrictions (16(4)(a)).	RELAXED
	Grace period increased for non-national security cases	5 working day grace period after change of circumstances becomes known (119(3)(c), (5)-(7))	RIPA	5 working days for national security, otherwise 1 working day. RIPA (16(4)(b), (5)-(6)) .	PARTIALLY RELAXED
	Replacement of RIPA 16(3) modification by targeted examination warrant.	Issue of targeted examination warrant (119(3)(d)). Cf Part 2 Chapter 1 (targeted examination warrants – interception).	RIPA	Modification of RIPA 8(4) warrant under 16(3). Anderson: 6.33, 6.50 to 6.51, 6.56(a), 6.57(c), 14.89 to	REPLACEMENT

				14.90, Recommendation 79. ISC: 112(iii), 113 to 115, Recommendation Q.	

Part 6 - Chapter 2 Investigatory Powers Draft Bill - Review of drafting provenance – Investigatory Powers Research Group. This working document may be subject to change, following further assessment. For abbreviations and full source list go to bit.ly/ipbillsources. Comments/suggestions to: ipbillresearchgroup@gmail.com.

IPB reference	Description of content	IPB extract	Source	Description in legislation / reviews	Issues/comments
s. 122	Awards SOS power to issue bulk warrants and outlines grounds on which those warrants may be issued.	The Secretary of State may … issue a bulk acquisition warrant if (a) the Secretary of State considers that the warrant is necessary (i) in the interests of national security, OR (ii) on that ground and on any other grounds falling within subsection (2)… (2) … (a) for the purpose of preventing or detecting serious crime, or (b) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security'	This entire chapter has no predecessor in RIPA. The use of these powers was only recently avowed and the legislative basis was given as s. 94 TA 84. All three reviews were critical of the lack of structure and oversight. The Government has now published non-statutory handling arrangements (relating to s. 94) which came into effect the day the draft IPB was published. Non-statutory guidance/ s. 94 refer to national security or international relations.		NEW. This might be a change in scope. It is not clear how grounds in subsection (2) relate to (1)(a)(ii). (2)(b) makes clear that economic interests should be linked to national security; (2)(a) does not do the same for serious crime, so it is unclear whether serious crime is a free-standing basis for a warrant. Note definitions in s. 195 – but this still allows some very broad general purposes to be identified. C.f. s. 125. Postal data seems to be excluded by s. 134.

122(3)		A warrant may be considered necessary on the ground falling within subsection (2)(b) only if the communications data which it is considered necessary to obtain is communications data relating to the acts or intentions of persons outside the British Isles	ISC reported that the external aspect needed clarifying.		This does not mean that people within the UK will be unaffected. Limitation also does not apply to 1(a) (i)/(2)(a).
122(4)		The matters to be taken into account in considering whether the conditions in paragraphs (a) and (b) of subsection (1) are met include whether the communications data which it is thought necessary to obtain under the warrant could reasonably be obtained by other means.	The new arrangements pertaining to s. 94 Telecommunications Act 1984 (TA) elaborate: 'whether there is a less intrusive method' and bearing in mind the level of 'collateral intrusion' (cl. 4.1.1).		S. 122(4) does not refer to collateral intrusion.
122(6)		The activities are (a) requiring a telecommunications operator specified in the warrant – (i) to disclose to a person specified in the warrant any communications data …specified.. . and is in the possession of the operator, (ii) to obtain any communications data specified .. which is not in the possession of the operator but which the operator is capable of obtaining, and (iii) to disclose to a person … any data, (b)	contains no detail on this point		A broader definition of 'telecommunications operator' makes this wider than s. 94 Telecommunications Act. This requires operators to obtain; does it require them to create? Note capabilities provisions in this regard.

		the selection for examination .. of communications data ..'			
122(8)		'A bulk acquisition warrant may relate to data whether or not in existence at the time of the issuing of the warrant'			This is forward looking, not just data already in existence. It is not clear whether this is in line with s. 94 TA (because s. 94 was vague). It matches analogous provisions in the rest of the bill.
s. 123	provides that warrants must be approved by judicial commissioner		This is new. S. 94 Telecommunications Act 1984 envisaged that the direction should be laid before Parliament. In practice this has not happened as. s. 94(4) allows for a national security exception. The new arrangement envisages that this exception will be relied upon as they state, the application must specify the national security grounds for not laying before Parliament.		The warrant does not envisage being laid before Parliament, but oversight is via the judicial commissioner.
123(2)	In so doing, the Judicial Commissioner must apply the same principles as				It is not clear what these standards might mean: see earlier comments.

	would be applied by a court on an application for judicial review'.				
s. 124	This provision states who takes the decision to issue the warrants.	'must be taken personally by the Secretary of State'	s. 94 Telecommunications Act – directions were given by the Secretary of State.		This seems functionally the same.
s. 125	Outline the information that must be contained in each warrant, including addressee and purpose	125(4) In specifying any operational purposes, it is not sufficient simply to use the descriptions contained in section 122(1)(a) or (2), but the purposes may still be general purposes'	This is new, but the handling arrangements emphasises that information must be given to allow assessment of necessity and proportionality.		
s. 126	Specifies initial duration of warrant	'A bulk acquisition warrant ceases to have effect at the end of the period of 6 months …'	s. 94 Telecommunications Act silent on duration. Handling arrangements specify 'Each intelligence Service must review, i.e. at intervals no less than six months …'; this is not the same as fixed term but may have the same effect, subject to possibility of renewal.		Note comments of ECtHR on possibility of repeat renewals in *Szabo and Vissy*. Are conditions (below) sufficient?

s. 127	Sets down the conditions on which warrants may be renewed	(1) If the renewal conditions are met, a bulk acquisition warrant may be renewed at any time before it would otherwise cease to have effect, by an instrument issued by the Secretary of State.	S. 94 Telecommunications Act silent. Handling arrangements do not envisage fix term with renewal but periodic review of justification (4.5.1-4.5.3). Oversight is by an internal review panel, subject to IOCC.		Conditions for renewal are that the grounds continue to exist and that the conduct continues to be necessary and proportionate. The decision is to be taken by the SoS and subject to review by JC. In this it seems to parallel the other provisions for renewal.
s. 128	Provides for the modification of warrants – the extent to which warrants may be modified and by whom	'The only modifications that may be made under this section are adding, varying or removing any operational purpose specified in the warrant as a purpose for which any communications data obtained under the warrant may be selected for examination'	THIS IS NEW		Modification is subject to comparable conditions as issue and renewal.
s. 129	provides the circumstances in which a warrant may or must be cancelled				There are no provisions as to how speedily the warrant stops or what to do with any data collected. (Cf *Zakharov*)
s. 130	Details the obligations of the addressee of the warrant and any others, including the fact that the obligation may be enforced through the civil courts.				

s. 131	Outlines restriction on the use of data and safeguards regarding unauthorised disclosure	131(2) …in relation to the communications data obtained … if each of the following is limited to the minimum that is necessary for the authorised purposes..- (a) the number of persons to whom any data is disclosed or otherwise made available, (b) the extent to which any of the data is disclosed or otherwise made available, (c) the extent to which any of the data is copied,(d) the number of copies that are made	Handling arrangements cross refer CESG Good Practice, plus obligations at 4.3.		Handling arrangements flag up sensitive categories: journalists, MPS, others. Note some references in s.131 to 'data' rather than 'communications data' – is this extending scope of protection (see general definition of data)? Note definition of 'copy' at subsection (10).
		131 (5) The requirements of this subsection are met in relation to the communications data obtained … if every copy made …. Is destroyed as soon there are no longer any relevant grounds for retaining it'	Handling arrangements s. 4.5.3		
s. 132	safeguards relating specifically to the examination (rather than acquisition) of data	(2) Examination of communications data is carried out only for the specified purposes if the data is examined only in so far as is necessary for the operational purposes	SOURCE: handling arrangements 4.3		
s. 133	creates the offence of disclosure of the existence of contents of the warrant without reasonable excuse	'It is an offence for – (a) a telecommunications operator who is under a duty by virtue of section 130 to assist in giving effect to a bulk acquisition warrant, or (b) any person employed for the purposes of the business of such an operator, to	THIS IS NEW		Non-disclosure offences apply throughout the act.

		disclose to any person, without reasonable excuse, the existence or content of the warrant			
s. 134	This contains some chapter specific definitions	'"communications data" does not include communications data within the meaning given by section 194(3)			This is different from the definition of 'communications data' elsewhere in this part.

Part 6 chapter 3 Investigatory Powers Draft Bill - Review of drafting provenance – Investigatory Powers Research Group. This working document may be subject to change, following further assessment. For abbreviations and full source list go to bit.ly/ipbillsources. Comments/suggestions to: ipbillresearchgroup@gmail.com.

IPB reference	Description of content	IPB extract	Source	Description in legislation/reviews	Issues/comments
s135(1)	Bulk equipment interference warrants: general	(1) For the purposes of this Act, a warrant is "bulk equipment interference warrant" if— (a) it is issued under this Chapter, (b) it authorises the person to whom it is addressed to secure interference with any equipment for the purpose of facilitating the obtaining of one or more of the following— (i) communications (see section 149); (ii) private information (see section 149); (iii) equipment data (see section 136); and (c) the main purpose of the warrant is facilitating the obtaining of one or more of the following— (i) overseas-related	Section 5 and 7 of the Intelligence Services Act 1994 and section 93 of the Police Act 1997. Note Code of Practice, 2015.	Guide to Powers and Safeguards (on face of draft bill) at page 16-17 says: Equipment interference is currently provided for under general property interference powers in the Intelligence Services Act 1994 and the Police Act 1997. A draft Code of Practice was published earlier this year and governs the use of equipment interference powers by the security and intelligence agencies. As some equipment interference techniques are used by all law enforcement agencies, the draft Bill will permit all police forces to undertake equipment interference; a Code of Practice will regulate the use of more sensitive and intrusive techniques. The draft Bill will create a new obligation on domestic CSPs to assist in giving effect to equipment interference warrants. Anderson report says:	Government states that bulk equipment interference is its attempt to "build on recommendations made by David Anderson QC and the ISC". The 2015 Code of Practice appears to have stretched the meaning of s. 7(4)(a) of the 1994 Intelligence Services Act's "acts of a description specified in the authorisation" to mean it covers bulk equipment interference. Section 7.11 of the Code of Practice claims s. 7(4)(a) "may relate to a broad class of operations". Part 6 Chapter 3 would appear to be aimed at codifying this in the new law.

		communications; (ii) overseas-related private information; (iii) overseas-related equipment data		There should be two types of bulk warrant: bulk interception warrants and bulk communication data warrants: Rec 42. Intelligence and Security Committee report says: Existing bulk interception is not indiscriminate, but involves a degree of targeting and filtering and they consider it essential for identifying threats.	
				IP Briefing Paper No 7371 says: Chapter 3: Bulk equipment interference warrants Clauses 135-149 deal with bulk equipment interference. Bulk equipment interference collects data relating to a number of devices; it is not targeted against particular persons, organisations or locations, or equipment that is being used for particular activities. Bulk equipment interference warrants are aimed at obtaining overseas related communications, private information or equipment data.	Main purpose of Chapter 3 bulk EI warrants seems intended to be facilitating hacking overseas related communications and equipment.

s135(2)	Contains definitions of overseas related terms	(2) In this Chapter — "overseas-related communications" means— (a) communications sent by individuals who are outside the British Islands, or (b) communications received by individuals who are outside the British Islands; "overseas-related private information" means private information of individuals who are outside the British Islands; "overseas-related equipment data" means equipment data that forms part of, or is connected with, overseas-related communications or overseas-related private information.	Undetermined	ISC suggested in relation to bulk warrants generally that the meaning of 'external communications' should be clarified: see Annex A, para O.	
s135(3)	Obtaining of communications, private information & equipment data via Equipment Interference	(3) A bulk equipment interference warrant may also authorise the person to whom it is addressed to secure— (a) the obtaining of any communications, private	New/Undetermined		This is one of the key sections in IP Bill facilitating hacking the internet. EI in bulk. Equipment data is defined in relation to Part 5 in cl 105, which refers back to cl 82. Equipment data for this part

		information or equipment data to which the purpose of the warrant relates; (b) the obtaining of any information that does not fall within paragraph (a) but is connected with the equipment to which the warrant relates; (c) the selection for examination, in any manner described in the warrant, of any material obtained under the warrant by virtue of paragraph (a) or (b); (d) the disclosure, in any manner described in the warrant, of any such material to the person to whom the warrant is addressed or to any person acting on that person's behalf.			is defined in cl. 136 in equivalent terms. See further below.
s135(4)	Authorisation of additional actions to aid bulk equipment interference	(a) any conduct which it is necessary to undertake in order to do what is expressly authorised by the warrant ….	New	Guide to Powers and Safeguards at front of draft bill notes: "The draft Bill will create a new obligation on domestic CSPs to assist in giving effect to equipment interference warrants".	S135(4)(a) seems to authorises *any conduct* necessary to secure information via bulk hacking. s135(4) appears to go beyond

					authorising just domestic CSPs to aid bulk EI. S135(4)(b) - On its face the wording authorises that *anyone* can do *anything* ("any conduct that is necessary") to help the bulk EI warrant holder get what they want.
s135(5)		(5) A bulk equipment interference warrant may not, by virtue of subsection (3)(a), authorise a person to engage in conduct, in relation to a communication other than a stored communication, that would (unless done with lawful authority) constitute an offence under section 2(1) (unlawful interception).			Safeguard appears circular but see also subsection (6) and note also limitation of use on bulk equipment interference warrants in cl 10 IPB. Note difference between real time and stored data. See definition in subsection (7).
s. 135(6)		(6) Subsection (4)(a) does not authorise a person to engage in conduct that could not be expressly authorised under the warrant because of the restriction imposed by subsection (5).			Seeks to prevent (4)(a) from being used to circumvent protection in (5).

s136(1)-(3)	Meaning of "equipment data"	(1) In this Chapter, “equipment data” means— (a) communications data (see section 193(5)); (b) data that falls within subsection (2) or (4).	Refer to interpretation of s. 193		"Equipment data" is any data connected with the functioning of any system (see (2) below); this is broad.
		(2) Data falls within this subsection if it identifies or describes anything connected with enabling or otherwise facilitating the functioning of a relevant system (including any apparatus in it) or of any service provided by means of the system.			
		(3) For the purposes of subsection (2), a system is a relevant system if any communications or private information are held on or by means of the system.			
s136(4)	Further meaning of equipment data	(4) Data falls within this subsection if, for the purposes of a relevant system, it is comprised in, included as part of, attached to or logically associated with a communication or an item	Undetermined - see previous use of general powers, and Code of practice		Meta data. The attempt in this part of the Bill to distinguish meta data from content. There is an increasing technical difficulty in separating communications data from content. Further, we might classify as

		of private information and either—(a) it does not form part of the content of the communication or the item of private information (see subsection (8)), or (b) if it does, it is capable of being logically separated from the remainder of the content in such a way that (after being separated)— (i) it would not reveal anything of what might reasonably be expected to be the meaning of the communication or item of information, disregarding any meaning arising from the fact of the communication or the existence of the item of information or from any data relating to that fact, and (ii) it would be data falling within subsection (5).			equipment or service or traffic or other meta data can in fact contain more valuable information than the content of communications.
s136(5)		(5) The data falling within this subsection is—	Undetermined		More meta data definitions - see also s. 193 IPB.
		(a) data which may be used to identify, or assist in identifying, any person, apparatus, system or			

		service; (b) data which may be used to identify any event;(c) data which may be used to identify the location of any person, event or thing			
		(6) For the purposes of subsection (5), the reference to data that may be used to identify any event includes— (a) data relating to the fact of the event;(b) data relating to the type, method or pattern of event; (c) data relating to the time or duration of the event.			
s136(8)		(8) For the purposes of this section, the content of a communication or an item of private information is the elements of the communication or item, and any data attached to or logically associated with it, which reveal anything of what might reasonably be expected to be the meaning of the communication or item, disregarding any	Undetermined		Definition of content which is unhelpful for the same reasons the meta data definitions are unhelpful. It is hard to maintain the distinction. This raises the question, however, of whether we believe there is no point distinguishing between content and communications attributes at all?

		meaning arising from the fact of the communication or the existence of the item or from any data relating to that fact.			
s137	Power to Issue Bulk Warrants - limitations in circumstances in which they may be issued	(a) the Secretary of State considers that the main purpose of the warrant is to facilitate the obtaining of overseas-related communications, overseas-related private information or overseas-related equipment data; (b) the Secretary of State considers that the warrant is necessary-(i) in the interests of national security or (ii) on that ground and on any other grounds falling within subsection (2) (f) the decision to issue the warrant has been approved by a Judicial Commissioner. (2) A warrant is necessary on grounds falling within this subsection if it is necessary— (a) for the purpose of	Undetermined but Judicial Commissioner warrant review provision is new	Reviews suggested that bulk warrants should be subject to judicial authorisation: RUSI Rec 8, Anderson Rec 46-48, ISC Annex A, paras F-M	Secretary of State has the power to issue bulk warrants, necessary and proportionate, on national security grounds, and for preventing/detecting serious crime or economic wellbeing of UK if in latter cases it is also related to national security. Secretary of State warrants get a procedural approval by a Judicial Commissioner. The procedure matches that with respect to bulk acquisition warrants - see also comments there.

		preventing or detecting serious crime, or (b) in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security.			
s137(3)		(3) A warrant may be considered necessary on the ground falling within subsection (2)(b) only if the interference with equipment that would be authorised by the warrant is considered necessary to facilitate the obtaining of material relating to the acts or intentions of persons outside the British Islands.	Undetermined -		Bulk EI warrants aimed at gaining information about actors located outside Britain.
s137(4)-(6)					Refers forward to cl. 140 procedural requirements for the bulk EI warrants. Cl 140(5) states specified "operational purposes" should be more clearly defined in a warrant than with a general reference to "national security", although warrant purposes

					may still be "general". The boundary between the two is not clear. This is the same as for other warrants. (See comments in *Zakharov* and *Szarbo and Vissy*).
s138(1)-(5)	Approval of Warrants by Judicial Commissioners		New		Judicial Commissioner is to carry out a judicial review type approval check on Secretary of State Bulk EI warrant. See comments on level of review in Part 2.
s139	Decision to issue warrants must be taken personally by Secretary of State	(1) The decision to issue a bulk equipment interference warrant must be taken personally by the Secretary of State	Undetermined		This follows the same approach as elsewhere for bulk warrants.
s139(1)-(5)	Requirements that must be met by warrants, including information it must contain	(4) A bulk equipment interference warrant must specify the operational purposes for which any material obtained under the warrant may be selected for examination			Procedural requirements for bulk EI warrants.
		(5) In specifying any operational purposes, it is not sufficient simply to use the descriptions contained in section 137(1)(b) or (2),			See above.

		but the purposes may still be general purposes.			
s141	Duration of Warrants	(1) A bulk equipment interference warrant ceases to have effect at the end of the period of 6 months …..	Undetermined		Warrants for bulk EI last for 6 months and can be renewed in 6 monthly rounds.
s142	Renewal of warrants	(1) If the renewal conditions are met, a bulk equipment interference warrant may be renewed, at any time before it would otherwise cease to have effect, by an instrument issued by the Secretary of State. Subsection 2 specifies renewal is conditional on the continuing existence of the conditions that justified the initial grant of the warrant	Undetermined		
					The bulk EI warrant can be renewed by the Secretary of State at any time during its operational period if the Secretary of State considers it continues to be necessary and proportionate. Renewals are subject to the approval of a Judicial Commissioner too. In this the review procedure

					follows the same lines as elsewhere in the draft bill.
s143	Modification of warrants	(2) The only modifications that may be made under this section are adding,varying or removing any operational purpose specified in the warrant as a purpose for which any material obtained under the warrant may be selected for examination	Undetermined		Secretary of State may modify an operational warrant - adding, varying or removing any operational purpose - if the SoS considers it necessary and proportionate. The modification must be approved by a Judicial Commissioner. The modification may only apply in such a way as it "does not affect the conduct authorised by it". A senior official acting on behalf of the Secretary of State may modify a live warrant if it involves removing any operational purpose of the warrant subject to a notification requirement in subsection (8).
s144	Cancellation of warrants - identifies when a warrant must be cancelled	(1) The Secretary of State, or a senior official acting on behalf of the Secretary of State, may cancel a bulk equipment interference warrant at any time. (2) If the Secretary of State, or a senior official acting on	s7 of the 1994 Intelligence Services Act		SoS or a senior official action on behalf of SoS may cancel a bulk EI warrant at any time and must cancel it if they consider it no longer necessary or proportionate.

		behalf of the Secretary of State considers, (a) that a bulk equipment interference warrant is no longer necessary in the interests of national security or, (b) that the conduct authorised by the warrant is no longer proportionate ... the person must cancel the warrant			
s145(1)-(2)	Implementation of warrants	(1) In giving effect to a bulk equipment interference warrant, the person to whom it is addressed ("the implementing authority") may (in addition to acting alone) act through, or together with, such other persons as the implementing authority may require (whether under subsection (2) or otherwise) to provide the authority with assistance in giving effect to the warrant.	Undetermined		Warrant holder may impose upon anyone to help give effect to the warrant: this potentially affects a broad class of persons.
s145(3)-(5)	Implementation of warrants continued	(3) A copy of a warrant may be served under subsection (2) on a person outside the United Kingdom for the	New	Guide to Powers and Safeguards in IP Bill page 16 notes: The draft Bill will create a new obligation on domestic	Bulk EI warrants requiring cooperation in giving effect to the warrant may be served on actors overseas. S. 145(3)

		purpose of requiring the person to provide such assistance in the form of conduct outside the United Kingdom.		CSPs to assist in giving effect to equipment interference warrants.	would appear to extend intent to create new obligation on domestic CSPs potentially to CSPs and other actors overseas.
		(4) Sections 100 (service of warrants) and 101 (duty of telecommunications providers to assist with implementation) apply in relation to a bulk equipment interference warrant as they apply in relation to a targeted equipment warrant …			
s146(2)-(3)	- relating to security of material and limitation of access to it	(3)(a) the number of persons to whom any of the material is disclosed or otherwise made available; (b) the extent to which any of the material is disclosed or otherwise made available; (c) the extent to which any of the material is copied; (d) the number of copies that are made.	Undetermined		SoS must ensure there are arrangements in place to minimise number of people who see bulk EI material & limit the extent to which is it disclosed and copied.
s146(4)	General safeguards continued	(4) For the purposes of subsection (3) something is necessary for the			Defines what is meant by "necessary" - if and only if it is necessary on the grounds of

		authorised purposes if, and only if—(a) it is, or is likely to become, necessary in the interests of national security or on any other grounds falling within section 137(2), (b) it is necessary for facilitating the carrying out of any functions under this Act of the Secretary of State, the Scottish Ministers or the head of the intelligence service to whom the warrant is addressed, (c) it is necessary for facilitating the carrying out of any functions of the Investigatory Powers Commissioner or of the Investigatory Powers Tribunal under or in relation to this Act, (d) it is necessary for the purpose of legal proceedings, or (e) it is necessary for the performance of the functions of any person by			national security, for example.

		or under any enactment.			
s146(5)	General safeguards continued	5) The arrangements for the time being in force under this section for securing that the requirements of subsection (3) are met in relation to the material obtained under the warrant must include arrangements for securing that every copy made of any of that material is stored, for so long as it is retained, in a secure manner.	Undetermined		Arrangements "for the time being" only? Must ensure material obtained is stored securely for as long as retained. Security of retained data will be critical and depend of the specifics of the arrangements.
s146(6)	General safeguards continued	(6) The requirements of this subsection are met in relation to the material obtained (6) The requirements of this subsection are met in relation to the material obtained under the warrant if every copy made of any of that material (if not destroyed earlier) is destroyed as soon as there are no longer any relevant grounds for retaining it (see subsection (7)).	Undetermined		If the retained data is destroyed immediately the grounds for retaining it expire that will fulfil safeguard requirements.

s146(7)	General safeguards continued	(7) For the purposes of subsection (6), there are no longer any relevant grounds for retaining a copy of any material if, and only if— (a) its retention is not necessary …in the interests of national security or on any other grounds falling within section 137(2), and (b) its retention is not necessary for any of the purposes mentioned in paragraphs (b) to (e) of subsection (4) above	Undetermined		No longer necessary to retain data unless there is a basis for doing so on grounds of national security or other grounds falling within cl. 137(2).
s146(8)	General safeguards-non-application to material outside the United Kingdom		Undetermined		If the data acquired through bulk EI has been handed over to foreign authorities (e.g. NSA?) protection actually secured is limited, but see cl 146(9).
s146(9)	General safeguards - equivalence of protection		Undetermined		SoS must ensure security arrangements are in force for materials handed over to foreign authorities but only if the intelligence service considers such safeguards appropriate. This follows the approach taken with regard to material derived from

					other types of warrant. The adequacy of protection is subject to the view of the Secretary of State.
s147(1)	Safeguards relating to examination of material	(1) For the purposes of section 146, the requirements of this section are met in relation to the material obtained under a warrant if— (a) any examination of the material obtained under the warrant is carried out only for the specified purposes (see subsection (2)), (b) the selection of any of the material for examination is necessary and proportionate in all the circumstances, and (c) where any such material is protected material, the selection of the material for examination meets any of the selection conditions (see subsection (3)).	Undetermined		Selection of retained bulk EI material for examination should be necessary and proportionate; and only for "specified purposes". Special arrangements for "protected material" which itself is defined in subsection (8) are in subsection (3).

s147(2)	Safeguards relating to examination of material	(2) Examination of the material is carried out only for the specified purposes if the material is examined only so far as is necessary for the operational purposes **….** In this subsection "specified" means specified at the time of the selection of the material for examination.	Undetermined		A bulk EI warrant must under cl. 140(4) specify the operational purposes for which any material obtained through the bulk hacking may be examined. This subsection appears to expand the definition of "specified" to mean purposes specified after the collection and retention of bulk EI data and just prior to examining it. A similar approach is taken with regard to other bulk warrants.
s147(3)-(4)	Safeguards relating to examination of material	(3) The selection conditions referred to in subsection (1)(c) are— (a) that the selection of the protected material for examination does not breach the prohibition in subsection (4); (b) that the person to whom the warrant is addressed reasonably considers that the selection of the protected material for examination would not breach that prohibition; (c) that the selection of the	Undetermined		"Protected material" [defined in subsection (8)] to be examined should not relate to an individual known to be in Britain at the time of the examination; or relating to contents of communications of such an individual. If a target, whether their identity is known or not, is in the UK should not use bulk EI data.

		protected material for examination in breach of that prohibition is authorised by subsection (5); (d) that a targeted examination warrant has been issued under Part 5 authorising the examination of the protected material. (4) The prohibition referred to in subsection (3)(a) is that the protected material may not at any time be selected for examination if— (a) any criteria used for the selection of the material for examination are referable to an individual known to be in the British Islands at that time, and (b) the purpose of using those criteria is to identify the content of communications sent by, or intended for, that individual or the content of private information			

		relating to that individual. It does not matter for the purposes of this subsection whether the identity of the individual is known.			
s147(5)-(6)	Safeguards relating to examination of material	(5) The selection of protected material ("the relevant material") for examination is authorised by this subsection if— (a) criteria referable to an individual have been, or are being, used for the selection of material for examination in circumstances falling within subsection (3)(a) or (b), (b) at any time it appears to the person to whom the warrant is addressed that there has been a relevant change of circumstances in relation to the individual (see subsection (6)) which would mean that the selection of the relevant material for examination would breach the prohibition in	Undetermined		Essentially this relates to examination of material related to an individual who enters the UK or the warrant holder was mistaken about the individual being outside the UK. So material collected that might relate to a suspect may be examined, if that suspect has, since the material was retained or during the operation of the bulk EI, entered the UK.

		subsection (4), (c) since that time, a written authorisation to examine the relevant material using those criteria has been given by a senior official, and (d) the selection of the relevant material for examination is made before the end of the permitted period (see subsection (7)). (6) For the purposes of subsection (5)(b) there is a relevant change of circumstances in relation to an individual if— (a) the individual has entered the British Islands, or (b) a belief by the person to whom the warrant is addressed that the individual was outside the British Islands was in fact mistaken.			
s147(7)	Safeguards relating to examination of material	(7) In subsection (5), "the permitted period" means the period ending with the	Derived from s 7.4 and s 7.14 of the		Intelligence agents get 5 days to examine bulk EI data

		fifth working day after the time mentioned in subsection (5)(b).	2015 EI Code of Practice		relating to a suspect known to have entered the UK.
s147(8)	Safeguards relating to examination of material	(8) In this section, “protected material” means any material obtained under the warrant other than— (a) equipment data, or (b) information connected with the equipment to which the warrant relates but that is not a communication, private information or equipment data.			Definition of "protected material" looks to have a broad scope.
s148	Application of other restrictions in relation to warrants under this Chapter	Section 102 (offence of making unauthorised disclosure) applies in relation to bulk equipment interference warrants as it applies in relation to targeted equipment interference warrants.	Undetermined		The s 102 offence referred to relates to making unauthorised disclosure. So anyone required to assist or to give effect to requirements of bulk EI warrant or activity is prohibited from disclosing it to anyone. Disclosure is a criminal offence unless permission to disclose is given by the bulk EI warrant holder.
s149	Chapter 3: interpretation	(1) In this Chapter— “communication” includes— (a) anything comprising	Undetermined		Broad definitions. So for example "equipment" effectively means "any device" with internet

		speech, music, sounds, visual images or data of any description, and (b) signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus; "equipment" means equipment producing electromagnetic, acoustic or other emissions or any device capable of being used in connection with such equipment; "equipment data" has the meaning given by section 136; "private information" includes information relating to a person's private or family life; "senior official" means a member of the Senior Civil Service or a member of the Senior Management			connectivity. Note implications for the internet of things.

		Structure of Her Majesty's Diplomatic Service. (2) References in this Chapter to the content of a communication or an item of private information are to be read in accordance with section 136(8). (3) References in this Chapter to the examination of material are references to the material being read, looked at or listened to by the persons to whom it becomes available as a result of the warrant.			
s135(1)	Bulk equipment interference warrants: general	(1) For the purposes of this Act, a warrant is "bulk equipment interference warrant" if— (a) it is issued under this Chapter, (b) it authorises the person to whom it is addressed to secure interference with any equipment for the	Section 5 and 7 of the Intelligence Services Act 1994 and section 93 of the Police Act 1997. Note Code of Practice.	Guide to Powers and Safeguards (on face of draft bill) at page 16-17 says: Equipment interference is currently provided for under general property interference powers in the Intelligence Services Act 1994 and the Police Act 1997. A draft Code of Practice was published earlier this year and governs the use of equipment interference powers by the security and	See comment for cl. 135(1) above.

		purpose of facilitating the obtaining of one or more of the following— (i) communications (see section 149); (ii) private information (see section 149); (iii) equipment data (see section 136); and (c) the main purpose of the warrant is facilitating the obtaining of one or more of the following— (i) overseas-related communications; (ii) overseas-related private information; (iii) overseas-related equipment data		intelligence agencies. As some equipment interference techniques are used by all law enforcement agencies, the draft Bill will permit all police forces to undertake equipment interference; a Code of Practice will regulate the use of more sensitive and intrusive techniques. The draft Bill will create a new obligation on domestic CSPs to assist in giving effect to equipment interference warrants. Anderson report says There should be two types of bulk warrant: bulk interception warrants and bulk communication data warrants. Intelligence and Security Committee report says Existing bulk interception is not indiscriminate, but involves a degree of targeting and filtering and they consider it essential for identifying threats	
				IP Briefing Paper No 7371: Chapter 3: Bulk equipment	Main purpose of Chapter 3 bulk EI warrants seems

				interference warrants Clauses 135-149 deal with bulk equipment interference. Bulk equipment interference collects data relating to a number of devices; it is not targeted against particular persons, organisations or locations, or equipment that is being used for particular activities Bulk equipment interference warrants are aimed at obtaining overseas related communications, private information or equipment data.	intended to be bringing hacking of overseas related communications and equipment within the statutory framework - both legitimising it but bringing it subject to some controls.

Part 7 Investigatory Powers Draft Bill - Review of drafting provenance – Investigatory Powers Research Group. This working document may be subject to change, following further assessment. For abbreviations and full source list go to bit.ly/ipbillsources. Comments/suggestions to: ipbillresearchgroup@gmail.com.

IPB reference	Description of content	IPB extract	Source	Description in legislation / reviews	Issues/comments
150(3)	definition of "personal data"	a set of information that includes personal data relating to a number of individuals'	Directions made under s. 59A RIPA (as amended by JSA 2013) placed the Intelligence Services Commissioner's oversight on a statutory basis, cross referring to the standards in s.2(2)(a) Security Service Act 1989, ss2(2)(a) and 4(2)(a) Intelligence Services Act 1994 ISC paras 151 - 163, Anderson, para 7.69	ISC: "Concerns remain particularly… with the revelation of bulk personal data sets which on the surface sound very much like an identity database…". See ISC Rec X. Directions define BPD as 'personal data as defined by s. 1(1) DPA 98'.	This is new in statute. Definition is extension of 'personal data' under DPA to include analogous data relating to dead people, so is broader than the definition under the Directions. Note that some Parts of the bill refer to 'personal information', with a different definition. The Explanatory memorandum states that the aim is to ensure datasets are not taken out of the purview of the system because they contain a few dead people (e.g. electoral roll). No distinction is made between personal data and sensitive personal data in DPA terms (c.f. Report of the Intelligence Services Commissioner for 2014), pp. 32-33
150(1)(b) and 150(2)(b)	definition of "bulk personal datasets"	"the nature of the set is such that it is likely that the majority of the individuals are not, and unlikely	Intelligence Services Commissioner	Directions at cl 5 define BPD as: 'any collection of	New in statute. This provision allows the security services to handle and process data sets

		to become, of interest to the intelligence service.."	(Additional Review) (Bulk Personal Datasets) Direction 2015	information which: comprises personal data as defined by section 1(1) of the Data Protection Act 1998; (b) relates to a wide range of individuals, the majority of whom are unlikely to be of intelligence interest; is held, or acquired for the purposes of holding, on one or more analytical systems within the Security and Intelligence Agencies.'	involving personal information of non-targets. Data sets in which individuals who are not of interest to the security services form the minority (but are still included) seem to fall outside the regime. The boundary between the data sets that fall inside the regime and outside it is the use of the term 'majority'. This seems to mean a data set of which 49% referred to persons not of interest to the security services would fall outside the regime. Reference to 'wide range' removed, allowing more narrowly focussed BPD to be included in the regime.
151	General provisions relating to the requirement for authorisation by warrant	"(1) An intelligence service may not exercise a power for the purpose of obtaining …(2) … to retain.. (3) to examine a bulk personal dataset ..unless.. Authorised by a warrant under this Part."	Intelligence Services Commissioner (Additional Review) (Bulk Personal Datasets) Direction 2015	4. 'The intelligence Services Commissioner must seek to assure himself that the acquisition, use retention and disclosure of bulk personal datasets does not occur except in accordance with section 2(2)(a) of the Security Service Act	The specific regime is new. Legality of previous system was based on a broad understanding of general powers. Warrants are required for each of the following acts: ss (1) obtaining BPD; ss (2) retaining BPD; and ss (3) examining BPD. The intention seems to be to exclude reliance on previously used general powers. Does this allow the sharing of the dataset with

				1989, sections 2(2)(a) and 4(2)(a) of the Intelligence Services Act.'	foreign agencies? The provision only applies to "intelligence service", defined s. 195 IPB. Warrants may be in relation to a class of BPD or an individual BPD (see 151(4)). Note Directions covered also 'disclosure'; this is not included in this regime. Does this mean disclosure is impermissible? There is no general prohibition or offence. See s. 19(3) Counter-Terrorism Act 2008
152	Exceptions to general requirement to have a warrant under this part of the act	"not apply to the exercise of a power conferred on an intelligence service by a warrant or other authorisation issued or given under this Act." (s152(1))			This allows the relevant services to rely on warrants granted under other parts of the act. The example given by the Explanatory Memorandum is where an interception warrant covers BPD, as well as intercept material.
		"not apply at any time when a bulk personal dataset is being retained for the purpose of enabling an application for a specific BPD warrant relating to the dataset to be made and determined." (s 152(2))			This allows a BPD to be retained before the warrant has authorised that retention; it refers to the requirement in 151(2) only so would not exempt the intelligence services from a warrant relation to obtaining (151(1)) or examining (151(3)). The Explanatory Memorandum gives a slightly different scenario

					suggesting it "allows intelligence agencies who have received unsolicited BPD or a BPD that falls outside an existing class BPD warrant to retain the dataset": both these examples are of acquisition so it seems as though on this interpretation 152(2) could limit 151(1) too.
		"..does not apply at any time when a bulk personal dataset is being retained or (as the case may be) examined for the purpose of enabling any of the information contained in it to be deleted."			The Explanatory Memorandum states '[i]f a warrant is cancelled or a specific warrant is not approved, it will not always be possible for the intelligence agency to delete it immediately from their systems. This provision allows the agencies to hold the BPD while they are ensuring that the relevant data is entirely removed from their systems." There is no time limitation to this, and query the scope of examination that is permitted. Recent decisions of the ECHR have taken note of national rules requiring deletion – see e.g. *Zakharov*.
153	Conditions on issuing class BPD warrants	"(1) The head of an intelligence service, or a person acting on his or her behalf, may apply to the			Why 'may'? Surely if the BPD falls within cl 150 then per 151 the intelligence service *must* apply?

		Secretary of State for a class BPD warrant." [See also 153(6) clarifying that a person acting for a head must hold office under the Crown.]			
		"(2) The application must include - (a) a description of the class of bulk personal datasets …., and (b) an explanation of the operational purposes for which the applicant wishes to examine bulk datasets of that class."			Same basic structure as for other warrants. See cl 162 on modification. Note case law of ECHR on ability of reviewing bodies to scrutinise necessity: e.g. *Zakharov*; *Szarbo and Vissy.*
		"(3)(a) the Secretary of State considers that the warrant is necessary (i) in the interests of national security, (ii) for the purposes of preventing or detecting serious crime, or (iii) in the interests of the economic well-being of the United Kingdom, so far as those interests are also relevant to the interests of national security,"	Intelligence Services Commissioners (Additional Review) (Bulk Personal Datasets) Direction cl 4 refers to SSA 1989 and SSA 1994	s. 2(2)(a) SSA 89: "The Director-General shall be responsible for the efficiency of the Service and it shall be his duty to ensure— (a) that there are arrangements for securing that no information is obtained by the Service except so far as necessary for the proper discharge of its functions or disclosed by it except so far as necessary for that	Grounds slightly broader that bulk acquisition warrants in that 153(3)(a)(ii) is not dependant on there being any national security issues; cl 122(2) grounds also require national security see 122(1)(a)(ii). No explanation of what 'necessary' might mean (c.f. 122(4)). Note comments of ECHR in e.g. *Zakharov*; *Szarbo and Vissy* Proportionality: see Report of Intelligence Commissioner, p. 36-7 - does this apply to BPD if the IPB comes in?

				purpose or for the purpose of the prevention or detection of serious crime or for the purpose of any criminal proceedings." Section 2(2)(a) ISA 94: "(a)that there are arrangements for securing that no information is obtained by the Intelligence Service except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary— (i) for that purpose; (ii) in the interests of national security; (iii) for the purpose of the prevention or detection of serious	

				crime; or (iv) for the purpose of any criminal proceedings"; s. 4(2)(a) ISA 94: "that there are arrangements for securing that no information is obtained by GCHQ except so far as necessary for the proper discharge of its functions and that no information is disclosed by it except so far as necessary for that purpose or for the purpose of any criminal proceedings".	
		"(3)(d) the Secretary of State considers that the arrangements made by the intelligence service for story bulk personal datasets of the class to which the application relates and for protecting them from unauthorised disclosure are satisfactory"	Intelligence Services Commissioner (Additional Review) (Bulk Personal Datasets) Direction 2015, cl 4	"… the Intelligence Services Commissioner must seek to assure himself of the adequacy of the Security and Intelligence Agencies' handling arrangements and	What level of security is required to satisfy "satisfactory" (as opposed to 'good' or 'secure')?

				their compliance therewith."	
		"(5) An examination that is not for an operational purpose specified in the warrant is not authorised by the warrant."			Some protection against "examination creep" (c.f cl. 152(3)). See comments in Report of Intelligence Service Commissioner 2014, p. 37.
154	definition of "specific BPD warrant"	Two cases arise: "(2) Case 1 is where-(a) the intelligence service wishes to obtain, retain and examine, or to retain and examine, a bulk dataset, and (b) the bulk personal dataset does not fall within a class described in a class BPD warrant. (3) Case 2 is where- (a) the intelligence service wishes to obtain, retain and examine, or to retain and examine, a bulk dataset, and (b) the bulk personal dataset falls within a class described in a class BPD warrant but the intelligence service at any time considers that it would be appropriate to seek a specific BPD warrant."			Both cases seem to envisage the possibility that the intelligence service has acquired a bulk personal dataset without a warrant. Other conditions the same as for class BPD warrants except that there is an 'urgent need' exception to the approval by judicial commissioner (cl. 154(5)(e)).
		"A specific BPD warrant relating to a bulk personal dataset … May also authorise …other bulk personal datasets … that do not exist at the time of the issue of			Only relates to a specific not a class warrant; two conditions: non-existence at time of warrant; and replacement, though it is not clear in whose opinion this is to

		the warrant but may reasonably be regarded as replacements…"			be seen as reasonable. See ss. 7(b) for warrant requirements in respect of replacements.
155	conditions to be taken into account by Judicial Commissioners when approving warrants				This is the same procedure as elsewhere - NB judicial review standard of consideration – note need for effective review according to both European courts.
156	Conditions for seeking to legitimise a warrant issued without judicial commissioner approval				This applies only in regards to specific warrants. Procedure the same as for targeted interception warrants – see comments there.
157	Consequences for warrants failing to get retroactive approval under 156	"(2) The head of the intelligence service to whom the warrant is addressed must, so far as reasonably practicable, secure that anything in the process of being done on reliance on the warrant stops as soon as possible".			Must stop retention/examination but subject to two possibly wide exceptions: 'practicality' and timing is 'as soon as possible' - both depend on interpretation. This is similar to the approach taken in analogous provisions elsewhere in the IPB.
		"(3) The Judicial Commissioner .. May (a) direct that any bulk datasets …be destroyed; (b) impose conditions as to the use or retention of any such datasets."			While the DPB may be destroyed, this provision allows material to be kept notwithstanding the fact that the warrant was not approved. Does this comply with ECHR standards: see discussions in e.g. *Zakharov.*
		"(8) Nothing …affects the lawfulness of - (a) anything done			Although the system envisages that judicial commissioner review

		in reliance on the warrant before it ceases to have effect" (see also 156(5)).			is required before the warrant is effective in urgent cases the position is reversed and the warrant is presumed effective until declared otherwise, which means actions before that point are and remain lawful; again there is a proviso about the practicality of stopping.
158	Requirement about who takes the decision about issuing a warrant	"(3) Before a specific BPD warrant is issued, it must be signed by the Secretary of State except that, in an urgent case, it may be signed instead by a senior official designated by the Secretary of State for that purpose. (4) Where a warrant is signed by a senior official, the warrant must contain a statement that the case is an urgent case in which the Secretary of State has personally expressly authorised the issue of a warrant."			Is there a system to check that the urgent cases are urgent? Here the check seems to be about who is making the decision, not whether the decision is urgent.
159	Information to be contained in warrants				Main point is whether the warrant is 'class' or 'specific', following the fact that there is a difference in treatment (urgent cases). Note importance of information for review of

					decisions according to the ECHR. Is this sufficient?
160	duration of warrants	"(2)(a) in the case of an urgent specific BPD warrant means the period ending with the fifth working day after the day on which the warrant was issued; (b) in any other case, means the period of 6 months….."			The Explanatory Memorandum states that these periods are consistent with the periods for other warrants under the IPB.
161	Information to be contained in warrants	"(2)(b) the conduct that would be authorised by the warrant continues to be proportionate…(c) ..(i) the examination that would be authorised continues to be necessary…"			The grounds and conditions for renewal reflect those for the grant but note the text refers to continued examination rather than just retaining the BPD.
162	provisions as to how a warrant may be modified and by whom	"(2) There are two kinds of modifications- (a) major modifications, and (b) minor modifications. (3) The major modifications that may be made are adding or varying any operational purpose specified in the warrant … (4) The minor modifications that may be made are removing any operational purpose ..."			The significance of the distinction is that more people may remove operational purposes than may add or vary: the minor corrections may be implemented by the head of the relevant intelligence service or a person who holds a senior position in that service (cl. 162(6)(c) and (d) and 162(7)). The grounds are the same as for the original warrant.
		"(10) Where a major modification of a …warrant is made by a senior official, the Secretary of State			For minor notifications the Home Secretary need not be notified; in fact there is no review process for

		must be notified personally of the modification and the reasons for making it"			minor modifications as they are essentially limiting surveillance that has already been authorised.
163	Specifies who can cancel a warrant and on what grounds	"(2) If any of the appropriate persons considers-(a) that a class BPD warrant or a specific BPD warrant is no longer necessary …., or (b) that the conduct authorised … is no longer proportionate to what is sought to be achieved by it, the person must cancel the warrant."			Cancellation is obligatory where either of the conditions in (2)(a) and (b) are met, though 'considers' is subjective. According to cl. 163(1) the cancellation may be at any time. Either the Secretary of State of a senior official may cancel a warrant. Consequences for activities under the warrant are in cl 164.
163	Conditions for the cancellation of a warrant				
164	Consequences for warrants where they have been cancelled or not been renewed.	"(3) The Secretary of State may - …. (b) with the approval of a Judicial Commissioner, authorise the retention or examination of any of the material, subject to such conditions as the Secretary of State considers appropriate."			The non-existence of a warrant does not automatically mean that the examination of BPD cannot be continued. While the retention is subject to Secretary of State's direction with JC approval, it is not clear whether this direction is subject to the conditions for first authorisation of the warrant, nor is it clear that the conditions that the Secretary of State imposes are subject to JC approval (or just the retention/examination of the material). A decision of the JC

					refusing to approve can then be referred to the Investigatory Powers Commissioner. The status of the BPD in the interim is not clear.

Part 8 Investigatory Powers Draft Bill - Review of drafting provenance – Investigatory Powers Research Group. This working document may be subject to change, following further assessment. For abbreviations and full source list go to bit.ly/ipbillsources. Comments/suggestions to: ipbillresearchgroup@gmail.com.

IPB reference	Description of content	IPB extract	Source	Description in legislation/reviews	Issues/comments
167(1)	Appointment of the Investigatory Powers Commissioner (IPC) and Judicial Commissioners by the PM.	The Prime Minister must appoint— (a) the Investigatory Powers Commissioner, and (b) such number of other Judicial Commissioners as the Prime Minister considers necessary for the carrying out of the functions of the Judicial Commissioners.	RIPA/Anderson (82), RUSI (10, 17).	Replacement of IOCCO, OSC & IS Commr by IPC. Number of Judicial Commissioners dependent upon PM's judgement: page 13 of the Impact Assessment suggests four will be needed.	1. No mention of deputy Investigatory Powers Commissioners or Inspectors (see IOCCO) although page 13 of the Impact Assessment suggests that there may be three. No equivalent to s63 RIPA (Assistant Surveillance Commissioners). 2. Note that under clause 167(7), IPC may delegate to any other Judicial Commissioner. 3. Will four Judicial Commissioners be sufficient when presumably one will have to be allocated to Scotland leaving only three in London?
167(2)	IPC & Judicial Commissioners must have held high judicial office.	unless the person holds or has held a high judicial office (within the meaning of Part 3 of the Constitutional Reform Act 2005)	RIPA (see for example s 57(5), although Bill does not mention being a	Requirement for Commissioners to hold/have held high judicial office.	

			member of the Judicial Committee of the Privy Council)/Anderson (104).		
167(6)-(8)	IPC also a Judicial Commissioner.	167(6): The Investigatory Powers Commissioner is a Judicial Commissioner and the Investigatory Powers Commissioner and the other Judicial Commissioners are to be known, collectively, as the Judicial Commissioners.		IPC is also a Judicial Commissioner (see cl 167(8)(a)) but not vice versa (unless delegation occurs under cl 167(7)). Note also cl 19(5) 'Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, refuses to approve a decision to issue a warrant under this Chapter, the person who made that decision may ask the Investigatory Powers Commissioner to decide whether to approve the decision to issue the warrant.'	1. Might this jeopardise appearance of independence if IPC also acting as Judicial Commissioner? 2. How would this affect IPC's review of warrants if involved in this process (see also comments on cl 169)? 3. Note ECtHR decision in *Zakharov* v *Russia* (para 280): commenting on the role of the Russian prosecutor's office, the court said 'This blending of functions within one prosecutor's office, with the same office giving approval to requests for interceptions and then supervising their implementation, may also raise doubts as to the prosecutors' independence.'
168	Terms and conditions of appointment of Judicial Commissioners	cl. 168(6): A Judicial Commissioner who is not the Investigatory Powers		Terms and conditions of appointment of Judicial Commissioners including IPC.	Seems important for Judicial Commissioners to be able to be dismissed if behave badly

	i.e. including IPC: 3 year appointment, removal before end of term only by resolution of each House of Parliament unless bankruptcy, disqualification as company director, order under Insolvency Act, conviction of an offence and receives sentence of imprisonment, or (for Judicial Commissioner who is not IPC) removal by the IPC on certain grounds after consultation with the PM.	Commissioner may be removed from office by the Investigatory Powers Commissioner on - (a) the ground of inability or misbehaviour, or (b) a ground specified in the Judicial Commissioner's terms and conditions of appointment.			but cl. 168(6) rather unspecific, with the action only requiring the IPC to consult with the PM. Does 'inability' mean physical or mental incapacity? Does 'misbehaviour' mean misfeasance? See also comments below on cl. 169(5)-(7) regarding possible blurring of constitutional lines.
169(1)-(4)	IPC's main oversight functions: exercise by public authorities of interception, acquisition/retention of communications data, equipment interference.	cl. 169(1): must keep under review (including by way of audit, inspection and investigation) the exercise by public authorities of statutory functions relating to - (a) the interception of communications, (b) the acquisition or retention of communications data, or (c) equipment interference.	cl. 169(1) Similar but not identical to s57 RIPA; cl. 169(4)(b) similar but not identical to s57(4A) RIPA.	Statutory functions expanded upon in cl. 169(2) to include disclosure, retention and other use of intercepted material and other data. Bulk datasets specifically mentioned as area for review in cl.169(3)(a).	1. cl. 169(1): is the Secretary of State a 'public authority'? (Assume 'yes' because of the definition in cl. 195 referring back to s6 of Human Rights Act). RIPA specifically mentions the exercise by the Secretary of State of his/her powers & duties. 2. Also, are the Judicial Commissioners 'public

					authorities' and so reviewable by the IPC? (again assume yes because of definition in cl. 195, and because Judicial Commissioners are not a court or tribunal (excluded by cl. 195)). But see also comments on cl 167(6) above. 3. Cl. 169(4)(e) excludes the exercise of any function which is subject to review by the Information Commissioner, but might there be overlaps e.g. regarding the retention of bulk datasets? 4. Should IPC have a specific function relating to the offences under the Bill e.g. unlawfully obtaining communications data in cl 8 of the Bill? 5. Should the IPC have the power to launch proactively inquiries or investigations into thematic matters/matters of public concern without needing a 'direction' from the PM?
169(5)-(7)	Judicial Commissioners must not prejudice	cl.169(7): Subsections (5) and (6) do not apply in relation to	cl. 169(5) reflects	As well as not prejudicing national security etc, Judicial Commissioners	1. Are there any other exceptions that should be

	national security, jeopardise the success of an intelligence operation etc, but this does not apply to deciding whether or not to approve a warrant.	the functions of a Judicial Commissioner of - (a) deciding whether to approve the issue, modification or renewal of a warrant or authorisation, (b) deciding what may be done with data or other material when a warrant issued for what was considered to be an urgent need is cancelled, or (c) reviewing any decision of the kind mentioned in paragraph (a) or (b).	statutory functions of intelligence services in SSA/ISA.	must not jeopardise the success of an operation or unduly impede an agency's operational effectiveness.	added to subsection (7) e.g. enabling the Judicial Commissioner to consult with other Commissioners, the IPC, expert advisers etc? 2. Concern has been raised (see evidence to Joint Bill Committee given on 7 December 2015 by Rt Hon Owen Paterson) that cl. 169(5)(6) will require Judicial Commissioners to make a 'political'/subjective operational decision outside normal constitutional roles. The consequences of 'breach' of these provisions seem unclear. Who would decide? Would it be grounds for removal for 'inability or misbehaviour' under cl. 168(6)?
170	Additional oversight functions for Investigatory Powers Commissioner.	cl. 170(4): The Prime Minister must publish, in a manner which the Prime Minister considers appropriate, any direction under this section (and any revocation of such a direction) except so far as it appears to the Prime Minister that such publication	cl. 170(1) = s59(A) RIPA; cl. 170(4) similar but not identical to s58(7) RIPA.	If directed by the PM, Investigatory Powers Commissioner must review other aspects of the functions of an intelligence service, its head (defined in cl. 195) or any part of the forces, or the Ministry of Defence engaging in intelligence activities. Directions to be	1. Are there other public bodies engaging in intelligence activities e.g. HMRC that should be included in cl. 170(1)? 2. Cl. 170(4) does not include obligation on the PM to consult with the IPC (as s.

		would be contrary to the public interest...		published except if PM believes would be contrary to public interest or national security etc.	58(7) of RIPA does) and appears to mean that the publication of the whole direction would be prevented, rather than particular material or matters being excluded. (Note importance given by *Zakharov* decision to public scrutiny of supervisory body and accessibility of reports (para 283).)
171	Investigatory Powers Commissioner to inform a person of relevant errors relating to that person provided the specified conditions are met, including the requirement that the error is 'serious' as defined (including that the error has caused serious prejudice or harm to the person, 171(3)) and it is in the public interest for the person to be informed. When a person is informed of an error, he/she must be	cl. 171(4): the fact that there has been a breach of a person's Convention rights (within the meaning of the Human Rights Act 1998) is not sufficient by itself for an error to be a serious error; cl. 171(11) "relevant error" mean an error - (a) by a public authority in complying with any requirements which are imposed on it by virtue of this Act or any other enactment and which are subject to review by a Judicial Commissioner, and (b) of a description identified for this purpose in a code of practice under Schedule 6...	Articles 6, 8 & 10 ECHR; Influenced by Special Advocate/SIAC (see *Chahal* v *UK*, 1996) or Public Interest Immunity claims? (Note that the court in *Zakharov* cited the decision in *Kennedy*: 'the absence of a requirement	New process says that a person must be informed by IPC of a relevant error relating to them if the IPC is aware of the error and considers that the error is serious AND the IPT agrees that it is serious, and considers that it is the public interest for the person to be informed of the error. In deciding on public interest, the IPT must consider the seriousness of the error, the effect on the person, and the extent to which disclosing the error would be contrary to the public interest or prejudicial to national security etc (171(5)).	1. There appears to be no 'ban' as such on disclosing an error even if the disclosure would be prejudicial to national security etc (under cl. 171(5)(b) the Tribunal only needs to have consideration to this) i.e. it could be prejudicial to national security to disclose but still in the public interest. Appears to be no scope for PII application by Secretary of State. Can therefore the Secretary of State JR/appeal the Tribunal if she wishes to challenge the disclosure decision? 2. Rule 47 of the SIAC Rules 2003 (as amended) relates to

	informed of any rights to apply to the Tribunal and be given such details as the IPC considers necessary for exercising those rights, having regard to public interest/national security considerations.		to notify the subject of interception at any point in time was compatible with the Convention, because in the UK any person who suspected that his communications were being or had been intercepted could apply to the Investigatory Powers Tribunal, whose jurisdiction did not depend on notification to the interception		where the reasons for the Commission's determination have not been fully disclosed because of public interest considerations. The Special Advocate is able to challenge that determination 'on the grounds that the separate determination contains material the disclosure of which would not be contrary to the public interest.' Is such a special advocate/amicus brief (or similar) process needed here to represent the interests of the potential disclosee in decisions as to whether the error has caused serious prejudice or harm and whether disclosure would be in the public interest? Note that if the IPC decides the error is not serious, then presumably the IPT never hears about it. 3. The definition of relevant error relates to requirements which are subject to review by a 'Judicial Commissioner' and would therefore seem to

			subject that there had been an interception of his or her communications.' (para 288))		include areas under the IPC's jurisdiction because of cl 167(6). 4. What if an error was wilful or reckless, but did not result in serious prejudice to the individual? Should this type of error also fall within the reporting regime?
174(6)-(7)	PM must publish the IPC's annual report and lay before Parliament including a statement as to whether any part has been excluded from publication.	174(7) The Prime Minister may, after consultation with the Investigatory Powers Commissioner, exclude from publication any part of a report under subsection (1) if, in the opinion of the Prime Minister, the publication of that part would be contrary to the public interest or prejudicial to - (a) national security...	Cl. 174(7) similar but not identical to s. 58(7) RIPA.	The exclusion of matters from the published annual report of the IPC.	1. No mention in this section itself of providing the report to the First Minister or laying before the Scottish Parliament (compare s. 58(6A) RIPA). 2. Wording of the Bill uses 'part of the report' rather than 'any matter in an annual report' in RIPA.
175(5)	Definition of relevant persons who must disclose 'documents and information' to a Judicial Commissioner.	"relevant person" means - (a) any member of a public authority, (b) any telecommunications operator or postal operator who is, has been or may become subject to a requirement imposed by virtue of this Act, or (c) any person who is, has been or may become subject to provide	Similar but not identical to s. 58(1) RIPA. Also see s. 68(7) RIPA.	Requirement for certain persons to disclose documents and information to Judicial Commissioners.	1. The definition of 'public authority' in cl. 195 would appear to incorporate persons holding office under the Crown. 2. The language of 'documents and information' needs updating to include direct access to technical systems and running queries.

		assistance by virtue of section 29, 31, 99, 101, 116, 130 or 145.			
176(2)	Resourcing of Judicial Commissioners.	as the Secretary of State considers necessary for the carrying out of the Commissioners' functions.	Similar but not identical to s. 57(7) RIPA/RUSI recommendation 18.	Provision for funding, staff, accommodation, equipment and other facilities.	Unlike RIPA (such resources 'as are sufficient' to enable the Commissioner to properly carry out his functions), resourcing is subject to the Secretary of State's opinion: that 'the Secretary of State considers necessary'. RUSI recommended that the IPC should have staff with technical, legal, investigative and other relevant expertise (e.g. in privacy and civil liberties). It is not clear whether the IPC would have access to the Technical Advisory Board (see cl. 183 of the Bill) which currently advises the Home Secretary, or would be able to consult lay persons e.g. via an ethics committee/advisory board.
177	Power to modify Commissioners' functions.	177(1): The Secretary of State may by regulations modify the functions of the Investigatory Powers Commissioner or any other Judicial Commissioner; (Note that Cl. 197(3) requires a		IPC's/Judicial Commissioner's functions can be modified by regulation.	Cl. 197(3) provides a legislative safeguard over the making of regulations under Cl. 177. See comments on the making of regulations.

		statutory instrument containing regulations under Cl. 177 to be laid before, and approved by, a resolution of each House of Parliament.)			
180	Creates a domestic right of appeal from decisions of the Investigatory Powers Tribunal (IPT) to the Court of Appeal (regulations will deal with Scotland and Northern Ireland) in cases where the IPT has made a determination and found there is a point of law at issue. Allows IPT decisions to be challenged domestically rather than having to go to the ECtHR.	New 67A(1) of RIPA: A relevant person may appeal on a point of law against any determination of the Tribunal of a kind mentioned in section 68(4) (other than a determination on a reference made to them by virtue of section 65(2)ca); New section 67A(3) An appeal may not be made without the leave of the Tribunal or, if that is refused, of the court which would have jurisdiction to hear it; New 67(A)4 The Tribunal or court must not grant leave to appeal unless it considers that - (a) the appeal would raise an important point of principle or practice, or (b) there is another compelling reason for granting leave.	Articles 6, 8 and 10, ECHR.	Inserts new section 67A into RIPA: domestic appeal from IPT on point of law.	1. Limited to appeals on a point of law. Leave to appeal required. 2. Although the Secretary of State (as respondent) or the public body involved would appear to be a relevant person in accordance with the new s. 67A(6), it is not clear that the Secretary of State could bring an appeal to the Court of Appeal relating to the new error reporting provisions, as that does not appear to be a determination of a kind mentioned in section 68(4) of RIPA.
182	Information Commissioner must audit Part 4 (retention of communications	The Information Commissioner must audit compliance with requirements or restrictions imposed by virtue of Part 4 in	Data protection principles.	Audit duty relevant in particular to the requirements on telecommunications operators in clauses 74 (data integrity and	This is potentially a huge task. Where are the additional resources for the ICO for this? Needs to be corresponding

	data) in relation to integrity, security or destruction of data retained.	relation to the integrity, security or destruction of data retained by virtue of that Part.		security) and 75 (disclosure of retained data) of the Bill.	obligations on CSPs to cooperate in a timely way with IC's audit requests, and power for IC to require an audit.

Part 9 Chapter 1 Investigatory Powers Draft Bill - Review of drafting provenance – Investigatory Powers Research Group. This working document may be subject to change, following further assessment. For abbreviations and full source list go to bit.ly/ipbillsources. Comments/suggestions to: ipbillresearchgroup@gmail.com.

IPB reference	Description of content	IPB extract	Source	Description in legislation / reviews	Issues/comments
s. 184	Brings schedule 7 into effect: schedule 7 contains rules regarding combined warrants. Sch 7 lists the possible combinations where a warrant may be issued for more than one form of surveillance, including surveillance covered by RIPA and s. 5 ISA 94.	cl. 9 Sch 7 'the law about [formalities] so far as relating to a warrant or other authorisation that may be included in a combined warrant, applies in relation to the part of a combined warrant that contains the warrant or other authorisation…' cl. 10(1) 'where Part 1 or 2 [of Sch 10] provides for a person to have power to issue a combined warrant, the person may issue a combined warrant containing any warrant or authorisation that may be included in it, whether or not that person would have power to issue that warrant, or give that authorisation, as a single instrument…'	The Explanatory Memorandum suggests that 'This builds on the existing ability to combine certain warrants and authorisations (RIPA allows authorisations that combine Property interference (under the Intelligence Services Act 1994) and Intrusive Surveillance).'		The draft IPB allows combined warrants in more circumstances than RIPA. Note also the effect of cl.10 to Sch 10, which may weaken control over persons who may issue warrants.

s.185	Provides for payments to be made towards some compliance costs	'The Secretary of State must ensure that arrangements are in force for securing that telecommunications operators and postal operators receive an appropriate contribution in respect of such of their relevant costs as the Secretary of State considers appropriate'	RIPA, s. 14	RIPA s14: 'receives such contribution as is, in the circumstances of that person's case, a fair contribution…'; s. 24(1) 'such arrangements are in force as he thinks appropriate for requiring or authorising …appropriate contributions towards the costs … in complying with notices under section 22(4)'	There is some cost recovery, but no guarantee as to total cost. The cost implications may be more than originally anticipated.
S. 186	Allows the Sos to pay for technology to be developed to facilitate surveillance.	The Secretary of State may – (a) develop, provide, maintain or improve, or (b) enter into financial or other arrangements … for the development….of, such apparatus, software, systems or other facilities or services as the Secretary of State considers appropriate for enabling or otherwise facilitating compliance by the Secretary of State …with this Act.			

s. 187	Amends the Intelligence Services Act 1994	187(1)(2)(a) 'In Section 3 (the Government Communications Headquarters)- (a) in subsection (1)(a), after 'monitor' insert 'make use of''	s. 3 ISA 94	s. 3 ISA 94: "(a)to monitor or interfere with electromagnetic, acoustic and other emissions and any equipment producing such emissions and to obtain and provide information derived from or related to such emissions or equipment and from encrypted material". According to the Explanatory Memorandum this amendment 'clarifies that GCHQ may ... make use of communications services in the manner in which it was intended they would be used. This could be used for public communications as well as for investigative purposes.'	Expands permitted activities of GCHQ in relation to this sort of equipment.

	(3) In section (5) (warrants: general)- (a) in subsection 92) omit 'subject to subsection (3) below', and (b) omit subsection (3)		s.5(3)	s.5(3) A warrant issued on the application of the Intelligence Service or GCHQ for the purposes of the exercise of their functions by virtue of section 1(2)(c) or 3(2)(c) above may not relate to property in the British Islands The Explanatory Memorandum says that this is to allow GCHQ to support the investigation of serious crime beyond supporting MI5.	This removes a limitation on GCHQ's activities.
s. 188	Allows Secretary of State to issue 'National Security Notices' s. 188	1) the Secretary of State may give any telecommunications operator in the United Kingdom a notice ("a national security notice") requiring the operator to take such specified steps as the Secretary of State considers necessary in the interests of national security'		The Secretary of State may, after consultation with a person to whom this section applies, give to that person such directions of a general character as appear to the Secretary of State to be necessary in the	Expanded application due to change in definition of telecommunications services. Safeguards have been introduced in respect of proportionality (sub section (2)) and non-avoidance of a warrant (subsection (4)), though this is limited to the 'main purpose'; incidental

		(4) but a national security notice may not require the taking of any steps the main purpose of which is to do something for which a warrant or authorisation is required under this act'		interests of national security or relations with the government of a country or territory outside the United Kingdom; S. 94(8) 'This section applies to….providers of public electronic communications networks".' The Explanatory Memorandum describes it as 'providing a new framework for obligations previously provided for under s.94 of the Telecommunications Act 1984'. Anderson suggested s. 94 was not of great importance (p. 100), but that there is little in the public domain about use of notices. According to Sir Anthony May's 2015 IOCCO Report at 2.1,	avoidance of a warrant by a notice seems permissible. There is no recourse to Judicial Commissioner.

				he has 'recently been asked by the Prime Minister and have agreed to formally oversee directions under Section 94 of the Telecommunications Act 1984'.	
s. 189	-	189(2): In this section 'relevant operator' means any person who provides, or is proposing to provide- (a) Public postal services, or (b) telecommunications services'		Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002 SI 2002/1931, made under section 12(1), (2) and (5), and by section 78(5) of the Regulation of Investigatory Powers Act 2000	Provision expanded due to changes in definitions; expanded because s. 12 RIPA dealt with interception warrants – there is no similar limitation here. Test for imposition of order is if SoS 'considers it is reasonable to do' subject to practicality. Note s.12 (11) RIPA contains some considerations regarding 'practical capability' which do not appear in cl. 189 IPB. Obligations are not defined exhaustively – contrast the closed list approach in 2002 order. Some examples in s. 189(4) reflect list in Schedule to 2002 Order e.g. 189(4)(c)

					reflects para 10 in the Schedule. There are questions about interpretation. An order can have an extraterritorial effect (subsection (8)), which is not mentioned in the 2002 Regulations
s. 190	Contains procedural and enforcement aspects regarding a national security notice or imposing technical capability requirements.	190 (3) Before giving a relevant notice, the Secretary of State must, among other things, take into account— (a) the likely benefits of the notice, (b) the likely number of users (if known) of any postal or telecommunications service to which the notice relates, (c) the technical feasibility of complying with the notice, (d) the likely cost of complying with the notice, and (e) any other effect of the notice on the person (or description of person) to whom it relates.	Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002 SI 2002/1931, made under section 12(1), (2) and (5), and by section 78(5) of the Regulation of Investigatory Powers Act 2000		Sub(s)(3) was not present in RIPA does not include a proportionality requirement. Subsection (11) refers back to subsections (9) and (10) which impose the obligation to comply, including in relation to those issues listed in (11) even if the person is outside the UK.

		190(11): technical capability notice is within this subsection if it relates to any of the following— (a) a targeted interception warrant or mutual assistance warrant under Chapter 1 of Part 2; (b) a bulk interception warrant; (c) an authorisation or notice given under Part 3			
s. 191	Allows for the notices to be review by the Secretary of State	(1) A person who is given a notice under section 188 or 189 may, within such period or circumstances as may be provided for in regulations made by the Secretary of State, refer the notice back to the Secretary of State (5) Before deciding the review, the Secretary of State must consult— (a) the Technical Advisory Board, and (b) the Investigatory Powers Commissioner.	Art 4 2002 Regulations		More detail than under RIPA/2002 Regulations. SoS must consult TAB and IPC but is not obliged to follow them.

192	Amendment of Wireless Telegraphy Act to avoid duplication	(2) Section 48 (interception and disclosure of messages) is amended as follows. (3) In subsection (1), for "otherwise than under the authority of a designated person" substitute "without lawful authority". (4) After subsection (3) insert— "(3A) A person does not commit an offence under this section consisting in any conduct if the conduct— (a) constitutes an offence under section 2 of the Investigatory Powers Act 2016 (offence of unlawful interception), or (b) would do so in the absence of any lawful authority (within the meaning of section 5 of that Act)." (5) Omit subsection (5). (6) Omit section 49 (interception authorities)	Wireless Telegraphy Act , s. 48, s.49	Wireless Telegraphy Act , s. 48 (1)A person commits an offence if, otherwise than under the authority of a designated person— (a) he uses wireless telegraphy apparatus with intent to obtain information as to the contents, sender or addressee of a message (whether sent by means of wireless telegraphy or not) of which neither he nor a person on whose behalf he is acting is an intended recipient, or (b) he discloses information as to the contents, sender or addressee of such a message. (2) A person commits an offence under this	

				section consisting in the disclosure of information only if the information disclosed by him is information that would not have come to his knowledge but for the use of wireless telegraphy apparatus by him or by another person. (3) A person does not commit an offence under this section consisting in the disclosure of information if he discloses the information in the course of legal proceedings or for the purpose of a report of legal proceedings.	

Part 9 Chapter 2 Investigatory Powers Draft Bill - Review of drafting provenance – Investigatory Powers Research Group. This working document may be subject to change, following further assessment. Comments/suggestions to: ipbillresearchgroup@gmail.com.

IPB reference	Description of content	IPB extract	Source	Description in legislation / reviews	Issues/comments
193(2)	Definition of "Communication", in relation to a telecommunications operator, service or system.	includes— (a) anything comprising speech, music, sounds, visual images or data of any description, and (b) signals serving either for the impartation of anything between persons, between a person and a thing or between things or for the actuation or control of any apparatus	RIPA s. 81(1) - identical; DRIPA was amended by CTSA 2015 s. (4)(a) to cite the RIPA definition.		Note definition of 'apparatus' in cl. 195.
193(3)	"Entity data" and "Events data" seem to replace the more prescriptive definition of "traffic data" in RIPA s21(6)	"Entity data" means any data which— (a) is about— (i) an entity, (ii) an association between a telecommunications service and an entity, or (iii) an association between any part of a telecommunication system and an entity, (b) consists of, or includes, data which identifies or describes the entity (whether or not by reference to the entity's location), and (c) is not events data.	New	Comments in ISC Report (at Rec V) refer to RIPA definition. See ISC Rec W.	Disclosure & filtering arrangements seem to cover *any* communications data, not just "traffic data" as under RIPA. Note definition of 'data' in cl. 195.

193(4)		“Events data” means any data which identifies or describes an event (whether or not by reference to its location) on, in or by means of a telecommunication system where the event consists of one or more entities engaging in a specific activity at a specific time.	New		
193(5)	Defines "communications data" for both data disclosure and data retention.	“Communications data”, in relation to a telecommunications operator, telecommunications service or telecommunication system, means entity data or events data—	Functionally equivalent to RIPA s. 21(4)	In this Chapter “communications data” means any of the following— (a) any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted; (b) any information which includes none of the contents of a	

				communication (apart from any information falling within paragraph (a)) and is about the use made by any person— (i) of any postal service or telecommunications service; or (ii) in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system; (c) any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or	

				telecommunications service.	
193(5)(a)	First group of 'communications data' is information that the operator does or [new] could obtain	(a) which is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator and—	Functionally equivalent to RIPA s. 22(4)	Text above.	The future tenses seem to indicate data that is not currently held or processed, so going beyond RIPA/DRIPA to allow ordering of collection of data the TSP does not need/generate/process.
193(5)(a)(i)		(i) is about an entity to which a telecommunications service is provided and relates to the provision of the service,	Replaces RIPA s. 21(4)(c), reducing scope to information "relating to the provision of the service"	Text above.	An improvement: previously it was anything else about the person held which could be very broad for example where the operator is a university or social network.
193(5)(a)(ii)		(ii) is comprised in, included as part of, attached to or logically associated with a communication (whether by the sender or otherwise) for the purposes of a telecommunication system by means of which the communication is being or may be transmitted, or	Replaces RIPA s. 21(4)(a) with additions.	Text above.	Adds data "included as part of" and "logically associated with" the communication. These are no longer limited to "traffic data" as in RIPA s. 21(6).
193(5)(a)(iii)		(iii) does not fall within sub-paragraph (i) or (ii) but does relate to the use of a	Replaces RIPA s. 21(4)(b)	Text above.	This seems functionally equivalent if "use by any person" is now "use".

		telecommunications service or a telecommunication system,			
193(5)(b)	Second group is the same types of data as (a), but "available directly from a telecommunication system".	(b) which is available directly from a telecommunication system and falls within sub-paragraph (i), (ii) or (iii) of paragraph (a), or	This may relate to RIPA s. 22(3) authorisations (Obtaining and disclosing communications data).		Implications unclear of including means of access within the definition of communications data.
193(5)(c)	Third group is about system architecture.	(c) which— (i) is (or is to be or is capable of being) held or obtained by, or on behalf of, a telecommunications operator, (ii) is about the architecture of a telecommunication system, and (iii) is not about a specific person, but does not include the content of a communication.	New		This seems a sensible thing to want but there wasn't previously a power to order its disclosure. It is not clear that this includes the NAT/PAT logs introduced into DRIPA by CTSA s. 21(3). If not, are they part of s. 71(9), 'relevant communications data'?
193(6)	Definition of "Content"	The content of a communication is the elements of the communication, and any data attached to or logically associated with the communication, which reveal anything of what might reasonably be expected to be the meaning of the communication but— (a) anything in the context of web browsing which identifies the	New - this has previously been left to the English language		It is unclear whether this changes the position from that in RIPA. Subsection (a) is presumably designed to tie in with ICRs, but the reference to 'web browsing' seems technology specific.

		telecommunications service concerned is not content, and (b) any meaning arising from the fact of the communication or from any data relating to the transmission of the communication is to be disregarded.			
193(7)	Definition of "Entity"	“Entity” means a person or thing.	New - unless from the same source as "entity data"		
193(8)	Definition of "Public Telecommunications Service"	“Public telecommunications service” means any telecommunications service which is offered or provided to the public, or a substantial section of the public, in any one or more parts of the United Kingdom.	RIPA s. 2(1)		
193(9)	Definition of "Public Telecommunications System"	“Public telecommunication system” means any parts of a telecommunication system by means of which any public telecommunications service is provided which are located in the United Kingdom.	RIPA s2(1)	"any parts" was "any such parts"	
193(10)	Definition of "Telecommunications Operator"	“Telecommunications operator” means a person who— (a) offers or provides a telecommunications service to	DRIPA s. 2(1) introduced the two part "provides"/"contr		"Preparatory" powers (filtering, retention, intercept facilities) apply to private systems/services/operators.

		persons in the United Kingdom, or (b) controls or provides a telecommunication system which is (wholly or partly)— (i) in the United Kingdom, or (ii) controlled from the United Kingdom.	ols" structure, but this adds "offers" and expands beyond public services/systems		Question whether DRIPA s. 2(1) is limited to public rather than including also private operators. DRIPA s2(1) recognises the existence of non-public networks, but the retention power in DRIPA s1(1) only applies to "a public telecommunications operator". A similar question could arise in relation to RIPA, s. 25(1). It provides that orders to provide telecommunications data under s. 21 RIPA can be made against private networks. This does not mean that all provisions in RIPA/DRIPA apply to public and private telecommunications operators. The Maintenance of Technical Capability in RIPA s. 12, for example, is limited to public telecommunications services. Under the Bill, the equivalents of DRIPA s. 1(1) and RIPA s. 12 seem to cover all telecommunications operators.
193(11)	Definition of "Telecommunications Service"	"Telecommunications service" means any service that consists	RIPA s. 2(1)		

		in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service).			
193(12)	"clarification", according to HMG that services such as webmail (and who knows what more) are included in "telecommunications service"	For the purposes of subsection (11), the cases in which a service is to be taken to consist in the provision of access to, and of facilities for making use of, a telecommunication system include any case where a service consists in or includes facilitating the creation, management or storage of communications transmitted, or that may be transmitted, by means of such a system.	DRIPA s. 5/RIPA s. 8A		Still unclear how far this definition stretches: Twitter, YouTube? It brings the definition closer to that used in the Budapest Convention, which may help to provide a limitation.
193(13)	Definition of "Telecommunication system"	"Telecommunication system" means a system (including the apparatus comprised in it) that exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy.	RIPA s. 2(1)	"a system" was "any system"; "that exists" was "which exists"	

193(14)	Definition of "Private Telecommunications System"	“Private telecommunication system” means any telecommunication system which— (a) is not a public telecommunication system, (b) is attached, directly or indirectly, to a public telecommunication system (whether or not for the purposes of the communication in question), and (c) includes apparatus which is both located in the United Kingdom and used (with or without other apparatus) for making the attachment to that public telecommunication system.	RIPA s. 2(1) with grammar changes		
194(2)	Definition of "Communication" for postal purposes	“Communication”, in relation to a postal operator or postal service (but not in the definition of “postal service” in this section), includes anything transmitted by a postal service.	RIPA s. 81(1)		
194(3)	definition of "Communications Data" for postal purposes	“Communications data”, in relation to a postal operator or postal service, means— (a) postal data comprised in, included as part of, attached to or logically associated with a communication (whether by the sender or otherwise) for the	RIPA s. 21(4)		

		purposes of a postal service by means of which it is being or may be transmitted, (b) information about the use made by any person of a postal service (but excluding the content of a communication (apart from information within paragraph (a)), or (c) information not within paragraph (a) or (b) that is (or is to be) held or obtained by a person providing a postal service, is about those to whom the service is provided by that person and relates to the service so provided.			
194(4)	Definition of "Postal Data"	“Postal data” means data which— (a) identifies, or purports to identify, a person, apparatus or location to or from which a communication is or may be transmitted, (b) identifies or selects, or purports to identify or select, apparatus through which, or by means of which, a communication is or may be transmitted, (c) identifies, or purports to identify, the time at which an event relating to a	RIPA s. 21(6) definition of traffic data		Adds "information included as part of" and "logically associated with".

		communication occurs, or (d) identifies the data or other data as data comprised in, included as part of, attached to or logically associated with a particular communication. For the purposes of this definition "data", in relation to a postal item, includes anything written on the outside of the item.			
194(5)	Definition of "Postal Item"	"Postal item" means— (a) any letter, postcard or other such thing in writing as may be used by the sender for imparting information to the recipient, or (b) any packet or parcel.	New		
194(6)	Definition of "Postal Operator"	"Postal operator" means a person providing a postal service to persons in the United Kingdom.	NOT the Postal Services Act 2011, though that does define the term		Bill definition presumably includes overseas operators.
194(7)	Definition of "Postal Service"	"Postal service" means a service that— (a) consists in the following, or in any one or more of them, namely, the collection, sorting, conveyance, distribution and delivery (whether in the United Kingdom or elsewhere) of postal items, and (b) has as its main purpose, or one of its main purposes, to make available, or	RIPA s. 2(1)		

		to facilitate, a means of transmission from place to place of postal items containing communications.			
194(8)	Definition of "Public postal operator"	“Public postal operator” means a person providing a public postal service.			
194(9)	Definition of "Public postal service"	“Public postal service” means a postal service that is offered or provided to the public, or a substantial section of the public, in any one or more parts of the United Kingdom.	RIPA s. 2(1)		
195(1)	Definition of "apparatus"	“apparatus” includes any equipment, machinery or device (whether physical or logical) and any wire or cable	RIPA s. 81(1)	“apparatus” includes any equipment, machinery or device and any wire or cable	Bill adds the phrase "whether physical or logical" to the RIPA definition, which seems to extend the scope of the definition. It is not clear whether this is just a recognition of virtual machines etc., or an attempt to include pure software providers. Note, the term is used in the Communications Act 2003, s. 32, and is distinguished from software.
196	Contains provisions relating to offences committed by corporate bodies or Scottish partnerships, including at ss. (2)		c.f s. 79 RIPA		

	attribution of offence to 'senior officers'				
197	elaborates on the powers of the secretary of state to make regulations (by statutory instrument). The provisions details the different procedures to be used in different categories of regulations: specifying that some regulations require 'enhanced affirmative procedure' (defined in s. 198) whilst others require affirmative procedure' or may be subject to annulment.		Cf RIPA s. 78. S. 78 RIPA referred to the negative procedures.		Note that the draft IPB envisages that there might be some 'Henry VIII' clauses. These are to be passed by affirmative procedure. There are specific provisions for the approval of codes under this act (see Schedule 6). The provisions here may be used where 'the provision could be included in regulations made under a different power conferred by this Act and subject to a different or no parliamentary procedure' (Cl. 197(8)). Note that SIs cannot, except in rare instances where the parent Act so provides or as permitted following Legislative and Regulatory Reform Act 2006, be amended or adapted by either House.
198	specifies the procedure by which the orders specified in s. 197(2) IPB are to be brought into force.	(2) Subsection (3) applies if—(a) the Secretary of State has consulted under section 56(2) in relation to making such regulations, (b) a period of at least 12 weeks, beginning with			The super-affirmative resolution procedure changes the rule that Statutory Instruments cannot be amended following being laid before Parliament so, as the

		the day on which any such consultation first began, has elapsed, and (c) the Secretary of State considers it appropriate to proceed with making such regulations. (3) The Secretary of State must lay before Parliament—(a) draft regulations, and (b) a document which explains the regulations. …. (6) The Secretary of State must have regard to—(a) any representations, (b) any resolution of either House of Parliament, and (c) any recommendations of a committee of either House of Parliament charged with reporting on the draft regulations, made during the 60-day period with regard to the draft regulations.			Explanatory Memorandum notes, the use of this procedure allows for greater scrutiny than the normal affirmative procedure. It applies to cl. 55, which deals with modifications to Sch.4 (public authorities with power under the IPB). The Explanatory Memorandum highlights that this means that 'there will be an enhanced scrutiny process should the Government wish to provide for additional authorities to be able to acquire communications data.' Subsection (3) requires that an explanatory document must accompany the draft, that – following subsection (2) the SoS has consulted and that the SoS has had regard to and representations under subsection (6).
199	Specifies that money to be spent under this act comes from that provided by Parliament.				

200	Bring Schedule 8 into force transitional, transitory and saving provisions. It also gives the SoS a power to make transitional regulations.				
201	Brings Sch 9 into force (minor and consequential provision).	(2) The Secretary of State may by regulations make such provision as the Secretary of State considers appropriate in consequence of this Act. (3) The power to make regulations under this section may, in particular, be exercised by modifying any provision made by or under an enactment.			This is a very broadly worded power. While it being in the same section as the minor and consequential provisions might suggest that it is linked to sch 9, it is not phrased in that way, and sub paragraph (3) suggests it may be used to amend an act (so a Henry VIII clause, potentially). It is a clause listed as requiring affirmative resolution under cl. 197 where it amends statute, that is it will be subject to heightened to scrutiny.
202	Describes the coming into force of the act. It may be brought into force gradually, by SI	(5) Her Majesty may by Order in Council provide for any of the provisions of this Act to extend, with or without modifications, to any of the British overseas territories.	s. 12 ISA	s. 12 ISA '(4)Her Majesty may by Order in Council direct that any of the provisions of this Act specified in the Order shall extend, with such exceptions, adaptations and modifications as	This is further potential for overseas effect.

				appear to Her to be necessary or expedient, to the Isle of Man, any of the Channel Islands or any colony'	

15 January 2016

Yahoo—written evidence (IPB0155)

Introduction

1. Yahoo welcomes the opportunity to submit written evidence to the scrutiny committee. Our company appreciates that governments must protect their citizens from terrorism and crime and safeguard individual rights (including the right to privacy) and liberties and economic growth. We understand that government surveillance can contribute to these objectives but powers to intrude on users' privacy must be lawful, proportionate, necessary, jurisdictionally bounded, and (to the maximum extent possible) transparent[1377].

2. It is hard to overstate the importance of this Bill not only in terms of establishing a clear and enduring domestic legal framework for the UK but also in terms of how it must interact with and complement legal structures in other countries and internationally. Moreover, decisions made today about UK legislation will set precedents which may be copied elsewhere and have wider ramifications for all parties, both in the UK and overseas. Our comments invite the Committee to consider (1) a wider context in which decisions about the Bill will be made and (2) the broader impact the Bill could have over time both in the UK and abroad.

About Yahoo

3. Yahoo was founded in 1995 on the principle that promoting access to information can improve people's lives and enhance their relationship with the world around them. Through our more than 20 years of international operations we recognise that our products, technology, and operating footprint increasingly intersect with human rights issues — and specifically, freedom of expression and privacy — around the world and that as a company, we have an obligation to engage responsibly, to respect the rights of our users and to promote the principles of free expression and privacy.

4. Our experiences as a pioneer in new markets led Yahoo to formally establish a dedicated Business and Human Rights Program (BHRP)[1378] in 2008, the first of its kind in the industry, in order to lead our efforts to make responsible decisions.

5. Yahoo is also a founding member of the Global Network Initiative[1379]. The GNI is a multi-stakeholder initiative of ICT companies, human rights organisations, academics, investors and others that works to protect and advance freedom of expression and privacy in the ICT sector. Through a process of stakeholder discussion, the GNI works to build consensus and has developed Principles of Freedom of Expression and Privacy and Implementation Guidelines[1380]. Yahoo has committed to these principles and guidelines, and Yahoo's BHRP serves to integrate the GNI Principles into our

[1377] See Reform Government Surveillance Principles, www.reformgovernmentsurveillance.com
[1378] See http://yahoobhrp.tumblr.com/post/75544734087/yahoo-business-human-rights-program-yahoo
[1379] See http://globalnetworkinitiative.org
[1380] See http://globalnetworkinitiative.org/implementationguidelines/index.php

business operations and decision-making. This integrated approach informs and shapes our engagement with governments around the world on authorised requests for data and on surveillance reform, including on the draft Investigatory Powers Bill.

6. The GNI Principles and Implementation Guidelines are complemented by an accountability mechanism whereby member companies agree to be assessed by a third-party assessor on the policies and procedures each company has in place to support their GNI commitments. A key part of this assessment focuses on a company's engagement with law enforcement and other government agencies, and also on company transparency with users about this engagement.

7. Yahoo has developed Principles for Responding to Government Requests for user data and content moderation. These Principles guide our efforts to balance our GNI commitments - which include engagement with governments regarding user privacy and free expression - with our public responsibilities and existing legal obligations, and inform our response to the imperfect international legal framework in which we operate. Information about this is publicly available in our Transparency Report[1381].

8. Yahoo is headquartered in Sunnyvale, California, and has offices located throughout the Americas, Asia Pacific (APAC) and the Europe, Middle East and Africa (EMEA) regions. Yahoo EMEA Ltd is registered in Ireland and operates under Irish law.

International context

9. Communications technology and services are increasingly cross-border, with many services now delivered globally from a single location. Users are also benefiting from a wide choice and increasingly consume digital services provided from outside their home jurisdiction. Lastly, law enforcement and security agencies increasingly have reason to request lawful access to data from other jurisdictions as the nature of the security threat also becomes more global.

10. This phenomenon creates a highly complex legal and operational environment for companies and agencies. It also creates a complex environment for users to navigate and establish their privacy rights. The current legal framework comprises the law in the requesting country, law in the receiving country and the international agreements that connect the two. Taken as a whole, this framework is fragmented, with gaps and conflicts which have gone unaddressed for many years. In this more global communications environment, this fragmentation has become more and more obvious and creates a patchwork of overlapping and conflicting laws which overseas and domestic UK CSPs must navigate in order to discharge their legal obligations to safeguard users' privacy and to respond appropriately to valid requests for access to data.

11. Another important contextual point arises from the UK's standing and influence around the world. There is strong anecdotal evidence that a number of overseas

[1381] See https://transparency.yahoo.com/

governments are watching this legislative reform process closely and intend to modify their domestic law in response. These are laws that will be used to request access to user data in other jurisdictions. It is therefore crucial that the draft Bill is worthy of emulation around the world by raising standards of privacy protections and serving as a model, particularly in countries where respect for international standards of human rights is not the norm.

12. The reviews led by David Anderson QC[1382] and Sir Nigel Sheinwald[1383] provided important time and space, away from the current security situation, to explore the international context and particularly the experiences of overseas providers receiving requests from UK agencies. Both reviews acknowledged the legal challenges and uncertainties companies and agencies face when interacting with different jurisdictions and concluded that more government-to-government engagement is required to modernize Mutual Legal Assistance Treaties (MLATs) and, where necessary, reach new international agreements. Modernised MLATs and new international mutual assistance agreements, paired with a framework that honours principles of proportionality and necessity, would create a sustainable and coherent echanism through which governments can lawfully pursue information held by foreign providers. This approach would fully engage foreign governments and other stakeholders, and establish high standards of authorization and oversight, as well as protecting the fundamental rights of users around the world from the extraterritorial over-reach of national surveillance laws, including users in the UK who use UK domestic CSPs. The Prime Minister has stated his support for this approach[1384].

Specific comments

Extraterritorial jurisdiction

13. In its current form, the draft Bill contains extraterritorial provisions that present a number of policy and legal concerns, and are highly problematic for overseas providers. With the inclusion of bulk powers for the first time, the extraterritorial jurisdiction in the draft Bill takes on new significance and is in effect *extended* to 7 of the 8 major powers – targeted lawful interception, targeted acquisition of communications data, mandatory retention of communications data, bulk lawful interception, bulk acquisition of communications data, targeted equipment interference and bulk equipment interference. Taken together, these powers broadly and *unilaterally* assert UK jurisdiction overseas.

14. The draft Bill provides inconsistent safeguards against unreasonable orders and warrants, and has limited safeguards from conflicts of law. In some cases, the powers are enforceable against overseas CSPs and in others against a UK entity of an overseas CSP which may not legally or operationally control user data for the

[1382] See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/434399/IPR-Report-Web-Accessible1.pdf
[1383] For summary, see https://www.gov.uk/government/news/special-envoy-on-intelligence-and-data-sharing-summary-ofwork.
[1384] HCWS27, 11 June 2015, see http://www.parliament.uk/business/publications/written-questions-answersstatements/written-statement/Commons/2015-06-11/HCWS27/

purposes of responding to access requests. Protections in some cases rely heavily on there being no offence for non-compliance, which provides limited comfort for overseas CSPs and creates an expectation of routine voluntary compliance outside international mutual assistance arrangements. There is also no affirmative obligation on the Secretary of State to notify or consult with overseas governments before exercising powers which may overlap with their domestic legislation. For example, the safeguards against a conflict of law seem to rely wholly on the Secretary of State's interpretation of foreign laws and all but two of the extraterritorial powers (targeted lawful interception and targeted acquisition of communications data[1385]) would operate *outside* the international mutual assistance framework recommended by David Anderson QC and Sir Nigel Sheinwald and enabled in the draft Bill. We set out these inconsistencies in the annex below.

15. We would point out to the Committee the likely longer term implications of the draft Bill even endorsing unilateral assertions of UK jurisdiction, ignoring the now explicit inclusion of bulk. This also touches on the Committee's questions around the *workability* of the draft Bill and how future proof it might be.

16. Extraterritoriality encroaches on the sovereign rights of other governments and risks retaliatory action, including against UK CSPs operating overseas. Broad extraterritorial powers in the draft Bill could create a chaotic international legal environment and unpredictability for companies, users and agencies and this impact would be greatly exacerbated if emulated by other governments. We know from past experience that some foreign governments will seek to enforce very intrusive surveillance laws against local operations of overseas companies and this places CSPs in a precarious position, including UK providers operating abroad.

17. This draft Bill has a complex set of goals to achieve. It must consolidate and clarify the UK legal framework, rebuild public confidence, and be both enduring and responsive to the demands of a global terrorist threat that could last decades. A new international legal framework is an essential complement to the draft Bill. New international agreements, however, require the support of a broad range of stakeholders and the ability to secure their support is directly linked to the provisions ultimately enacted in the Bill. It is our view that the extensive unilateral extraterritorial powers in the draft Bill are incompatible with this broader goal. There is a concern that it will distract from, and over time undermine, efforts to develop a clear, coherent and predictable international legal framework for users, companies and agencies. Decisions taken in respect of the Bill send a powerful message and thus also risk impacting the free flow of data, innovation and economic growth by discouraging investment in the UK in the longer term.

18. It is also worth noting that the UK government's position on extraterritoriality has in the past acknowledged that RIPA had no jurisdiction over overseas providers[1386].

[1385] It is, however, unclear whether international mutual assistance arrangements would be the default, or exclusive, mechanism for UK agencies to lawfully obtain targeted intercept and communications data from overseas services.
[1386] *Protecting the Public in a Changing Communications Environment*, April 2009. The Home Office said in this consultation *"And overseas companies outside UK jurisdiction are not required to disclose data under RIPA and not required to retain the data under the EU Data Retention Directive"*, p19.

However, in proposing DRIPA in 2014, government asserted that RIPA was always intended to apply extraterritorially.

19. Independent of the Committee's assessment of whether the powers themselves are proportionate and necessary (see other comments below), we would urge the Committee to:

- **reconsider the broad unilateral assertion of UK jurisdiction extraterritorially, bearing in mind the likely implications for the coherence of the international legal framework with which companies, agencies and users must interact;**
- **place the longer-term goal of a more coherent international legal framework at the heart of the Bill by explicitly extending the international mutual assistance arrangements to all powers;**
- **strengthen safeguards, *within these arrangements*, by ensuring the exercise of powers is subject to *separate* tests for reasonableness and conflicts of law. These safeguards must be consistent across all powers;**
- **remove inconsistent approaches to the serving of warrants on overseas CSPs, to ensure that warrants can only be served on an entity which has legal and operational control of user data for the purposes of responding to lawful requests for access, and clarify that the Bill authorizes UK agencies to *request* information from overseas CSPs acting under their applicable law rather than *compel* them under UK law.**

Mutual Legal Assistance Treaties

20. The Committee specifically invites comments on how well the current process under MLATs works for the acquisition of communications data.

21. MLATs are government-to-government treaties which are defined and resourced by governments. They provide an important legal process for dealing with cross-border requests for lawful access to data in another jurisdiction and due process for users whose privacy and other fundamental rights are in question. MLATs, and agreements like them, are crucial elements of the legal framework for overseas CSPs and their users. They continue to be an important mechanism for agencies to lawfully acquire data for investigations.

22. It has been acknowledged for some time that MLAT processes have not kept pace with the rise in demand as communications services, user behaviour and security threats have become more global. This is a known problem and, in response to parliamentary scrutiny of the draft Communications Data Bill, we understand that the Home Office has invested in the modernization of its MLAT processes. Yahoo fully supports this reform and, along with peer companies, has advocated for modernization and more resourcing in the US in order to streamline the UK-US MLAT process[1387].

[1387] Congress passed an omnibus spending bill on 18 December 2015, which included an additional US$32.1m for the Dept for Justice for MLAT reform. This is in addition to funding approved in the Appropriations Bill in November 2014.

23. Sir Nigel Sheinwald acknowledged the challenges around MLATs and this is why he recommended that government take a leadership role in modernizing existing MLATs and negotiating new international agreements, where necessary. We support this objective but, as noted above, there is a concern that the draft Bill could put at risk this unique opportunity to develop a clear and coherent international legal framework and safeguard the fundamental rights of users around the world.

24. We therefore urge the Committee endorse the recommendations above.

Judicial authorisation

25. We welcome the UK Government's commitment to move to a system of judicial authorization for lawful requests to access content, including lawful interception.

26. The Committee will be mindful that the UK has a responsibility to uphold international standards and, as noted above, Government's commitment also bears on its ability to engage other governments to address shortcomings in the international legal framework. To be consistent with prevailing international standards and meet the test set out by David Anderson QC in his review, however, judicial authorization should not be limited to judicial review principles (clause 19).

27. **We would therefore invite the Committee to make the following recommendations:**

- **subject applications for warrants to a distinct and independent prior evaluation by the judiciary, akin to the rigorous "probable cause" requirements under U.S. law;**
- **require major modifications (clause 26) to receive prior authorisation of a judicial commissioner and require minor modifications to be notified to a commissioner.**

Oversight

28. We very much welcome the Government's commitment to create world leading oversight in the UK.

29. Greater detail on the face of the Bill around what CSPs can expect from the new mechanism would provide valuable reassurance and clarity. **We would therefore invite the Committee to:**

- **support the inclusion of an affirmative obligation on the Investigatory Powers Commissioner to hear complaints from CSPs (including overseas CSPs) about the interpretation of the law and that these legal interpretations are transparent to all CSPs;**
- **ensure that the new body be better resourced, as well as have access to (and utilise) independent expert technical and legal advice in order to be effective and build public confidence in the exercise of surveillance powers;**
- **endorse the addition of further detail around the responsibilities and operation of the Investigatory Powers Commission on the face of the Bill.**

User transparency

30. As noted above, user transparency around engagement with law enforcement and government agencies is a key component of company accountability to users. It is also a prerequisite of redress and complements the goal of creating world-leading oversight. We welcome the Government's commitment to greater transparency.

31. The Regulation of Investigatory Powers Act 2000 ("RIPA") contains an offence of "tipping off" which creates legal ambiguity around companies' ability to inform users when their data has been lawfully requested by an authorised agency. CSPs, and other stakeholders, have an interest in the draft Bill putting it beyond doubt that companies can be transparent with their users, with appropriate limitations for operational purposes (e.g.: delayed notice where an investigation is ongoing).

32. In the draft Bill, it would be a "reasonable excuse" (clause 66(2)) for a CSP to provide user notice but only with permission of the relevant public authority. CSPs would not be permitted under any circumstances to disclose a lawful interception of a user's communications. Indeed, it would be a criminal offence to make a disclosure in respect of targeted interception warrants (clause 43 & 44), as well as for acquisition of communications data (clause 66), retention notices (clause 77(2)), equipment interference (clause 101 & 102), bulk interception (clause 120(2)) and bulk acquisition of communications data (clause 133).

33. We would encourage the Committee to:

- **support an approach whereby the default position is that the user can be notified by the provider or the requesting agency in advance of disclosure, unless delayed notice is required to preserve the integrity of an investigation;**
- **support a disclosure mechanism for lawful interception and other powers;**
- **clarify that the offences for disclosure do not preclude CSPs obtaining legal advice from external counsel, as currently provided for in RIPA s19(9).**

Bulk powers

34. It is to be welcomed that Government has set out the recently avowed powers currently available to UK agencies in the draft Bill so that the UK parliament and the public have an opportunity to debate them.

35. In its scrutiny, the Committee must be mindful that the term "bulk" has evolved to mean different things to different stakeholders and that, through the process of legislative reform, it now has a different legal meaning in different jurisdictions.

36. In the US for example, the USA Freedom Act ended bulk collection of internet data under the PATRIOT Act s215, the FISA pen register authority, and national security

letter statutes. It also now prohibits large-scale, indiscriminate collection, such as all records from an entire state, city, or zip code.

37. The Committee should also note that, although some enabling legislation for US national security surveillance may appear quite broad (s702 FISA), the authorized collection requires specifically identified targets.

38. The bulk powers in Parts 5 and 6, however, are significantly more extensive and their impact is exacerbated by the intention to bring all powers within a single Bill. For example, while the USA Freedom Act disavowed the bulk collection of communications data under an ambiguous statutory authorization, the draft Bill *explicitly* authorizes more intrusive bulk collection. The draft Bill also appears to apply all bulk powers to all services i.e.: over-the-top, network infrastructure and fixed and mobile telecommunications services via the broader definition of "telecommunications service" (clause 193(11)). Moreover, the powers explicitly apply extraterritorially to overseas services and as such could create a new conflict of law for some providers. The Bill provides some defences but they provide limited legal comfort and these powers will almost certainly be emulated by other countries, creating a new layer of complexity in the international legal framework.

39. Bulk powers are by definition very intrusive and indiscriminate. It is important that the Committee goes beyond merely placing bulk powers on a firmer statutory footing but also scrutinizes their proportionality and necessity. Many of the powers were envisioned many years ago and, as the UN special rapporteur observed, *"outdated domestic laws that were designed to deal with more rudimentary forms of surveillance have been applied to new digital technology without modification to reflect the vastly increased capabilities now employed by some States"*[1388]. The Committee should be mindful that scrutiny in other legislatures has focused on the utility of bulk powers and has accordingly led to a narrowing of powers where their proportionality and necessity has been re-evaluated.

40. **In addition, we would urge the Committee to:**

- **endorse the view that unilateral extraterritorial powers should end and extend the international mutual assistance arrangements to all powers;**
- **recommend providing greater clarity by more explicitly and narrowly defining bulk powers and being specific about when they would be exercised and to which communications (i.e.: specific types of "communications services" or all) they would apply;**
- **oppose provisions which could enshrine new conflicts of law for overseas providers;**
- **recommend the provision of safeguards against over-use of the most intrusive powers and 'power of last resort' wording.**

Misc provisions

[1388] Fourth annual report submitted to the UN General Assembly by the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Ben Emmerson, para 37

41. Clause 189 contains a very broad power for the Secretary of State to require a CSP to maintain certain technical capabilities with respect to targeted interception, targeted acquisition of communications data and bulk interception. This is far broader than the equivalent power under RIPA (which is limited to targeted interception in s12). This power also has extraterritorial effect and as such could be applied to overseas CSPs, with no safeguards on the face of the Bill for conflicts of law.

42. This is an extremely broad power and could prospectively limit a company's ability to meet other legal obligations to protect their users' privacy and keep their services secure from intrusion. For example, a notice could significantly constrain CSPs' ability to keep their users and infrastructure secure, and conflict with existing legal obligations on CSPs under other statutes (e.g.: Data Protection Directive, ePrivacy Directive).

43. We would urge the Committee to make the following recommendations:

- **provide reassurance on the face of the Bill that there is no conflict with CSPs' statutory obligations to keep user data and infrastructure secure;**
- **introduce statutory provisions recognising the importance of network integrity and cyber security;**
- **require agencies acting under equipment interference powers to inform companies of vulnerabilities that may be exploited by other actors.**

Annex

Extraterritorial jurisdiction powers in draft Investigatory Powers Bill

Provision	ETJ applies	Reasonableness test	Conflict of laws defence	Enforceable against overseas CSP	International mutual assistance framework	Obligation on SoS to consult CSP
Targeted interception Clause 29(4)	Yes	Yes Clause 31(5)	Yes Clause 31(5)	Yes Clause 31(8)	Yes	No
Targeted acquisition of comms data Clause 69	Yes	Yes Clause 69(4)	Yes Clause 69(4)	Yes Clause 50(4)	Yes	No
Mandatory data retention	Yes	Partial[1389]	No[1390]	No	No	Yes Clause 72(2)
Targeted equipment interference Clause 99(3)	Yes	Yes Clause 102(6)	No[1391]	No	No	No

[1389] There's no explicit reasonableness test in this section but Clause 72(1) cover some of this ground.
[1390] Confusing as there is no explicit offence for failure to comply.
[1391] Ibid.

Bulk interception Clause 116(3)	Yes	Yes Clause 116(5)	Yes Clause 116(5)	Yes Clause 116(5)	No	Yes Clause 108(2)
Bulk acquisition of comms data Clause 130(3)	Yes	Yes Clause 130(5)	Yes Clause 130(5)	Ambiguous[1392]	No	No
Bulk equipment interference Clause 145(3)	Yes	Yes Clause 145(4)	No[1393]	No	No	No
Bulk personal data sets Clause 150	No	-	-	-	-	-
Technical capability notice Clause 189	Yes	Partial[1394]	No	Partial[1395]	-	Yes Clause 190(2)

21 December 2015

[1392] Clause 130(6) could be aimed at UK CSPs only or also include local subsidiaries of overseas CSPs
[1393] See fn 11
[1394] Clause 130(3) is limited to technical feasibility and cost, not broader "reasonably practicable" test as in Clause 31
[1395] If the notice relates to an enforceable power, then the notice is also enforceable – see Clause 190(10) and 190(11)